

Software Maintenance Release Note

Maintenance Version 291-19

for AR415S, AR440S, AR441S, AR442S, AR450S, AR725, AR745, AR750S, AR750S-DP, and AR770S routers and AT-8600, AT-8700XL, Rapier i, Rapier w, AT-8800, AT-8900, x900-48, AT-9900, and AT-9800 Series switches

This software maintenance release note lists the issues addressed and enhancements made in Maintenance Version 291-19 for Software Version 2.9.1. Version details are listed in the following table:

Models	Series	Release File	Date	Size (bytes)	GUI file
AR415S, AR440S, AR441S, AR442S, AR450S	AR400	54291-19.rez	19 February 2009	4995992	415s_291-19_en_d.rsc 440s_291-19_en_d.rsc 441s_291-19_en_d.rsc 442s_291-19_en_d.rsc 450s_291-19_en_d.rsc
AR750S, AR750S-DP, AR770S	AR7x0S	55291-19.rez	19 February 2009	4115952	750s_291-19_en_d.rsc (AR750S and AR750S-DP)
AR725, AR745	AR7x5	52291-19.rez	19 February 2009	4115952	_725_291-19_en_d.rsc _745_291-19_en_d.rsc
AT-8624T/2M, AT-8624PoE, AT-8648T/2SP	AT-8600	sr291-19.rez	19 February 2009	2518372	8624t_291-19_en_d.rsc 8624poe_291-19_en_d.rsc 8648t_291-19_en_d.rsc
AT-8724XL, AT-8748XL	AT-8700XL	87291-19.rez	19 February 2009	2430152	8724_291-19_en_d.rsc 8748_291-19_en_d.rsc
Rapier 24i, Rapier 48i, Rapier 16fi	Rapier i	86291-19.rez	19 February 2009	4625608	r24i_291-19_en_d.rsc r16i_291-19_en_d.rsc r48i_291-19_en_d.rsc

Models	Series	Release File	Date	Size (bytes)	GUI file
Rapier 48w	Rapier w	86291-19.rez	19 February 2009	4625608	-
AT-8824, AT-8848	AT-8800	86291-19.rez	19 February 2009	4625608	8824_291-19_en_d.rsc 8848_291-19_en_d.rsc
AT-8948, AT8948i, x900-48FE, x900-48FE-N, x900-48FS	x900-48	89291-19.rez	19 February 2009	4918932	-
AT-9924T, AT-9924SP, AT-9924T/4SP	AT-9900	89291-19.rez	19 February 2009	4918932	9924_291-19_en_d.rsc
AT-9812T, AT-9816GB	AT-9800	sb291-19.rez	19 February 2009	4016740	9812_291-19_en_d.rsc 9816_291-19_en_d.rsc

Caution: Using a maintenance version on the wrong model may cause unpredictable results, including disruption to the network.

This maintenance release note should be read in conjunction with the following documents:

- the Release Note for Software Version 2.9.1, available from www.alliedtelesis.co.nz/documentation/relnotes/relnotes.html, which describes the new features since Version 2.8.1
- your router or switch's Document Set for Software Release 2.9.1. This document set is available on the CD-ROM that shipped with your router or switch, or from www.alliedtelesis.co.nz/documentation/documentation.html

Caution: Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in or omissions arising from the use of this information.

Enabling and installing this version

To use this maintenance version you must have a base release license for Software Release 2.9.1. Contact your distributor or reseller for more information about licences. To enable this version and install it as the preferred version, use the commands:

```
enable rel=xx291-19.rez num=2.9.1
set install=pref rel=xx291-19.rez
```

where *xx* is the prefix to the filename, as shown in the table on page 1. For example, to install the version on an x900-48FE switch, use the commands:

```
enable rel=89291-19.rez num=2.9.1
set install=pref rel=89291-19.rez
```

Levels

Some of the issues addressed in this maintenance version include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

- Level 1** This issue will cause significant interruption to network services, and there is no work-around.
- Level 2** This issue will cause interruption to network service, however there is a work-around.
- Level 3** This issue will seldom appear, and will cause minor inconvenience.
- Level 4** This issue represents a cosmetic change and does not affect network operation.

Features in 291-19

Software Maintenance Version 291-19 includes the resolved issues in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-19 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023546	Spanning Tree Protocols	2	STP forwarding did not operate correctly between switches connected with an aggregated link. This could have caused ports in the link to be in the discarding state, rather than the forwarding state. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00023702	Firewall	2	The add firewall policy httpfilter command allows you to specify a file containing a list of commands to control web access. However, the keyword aspect of this control file was not filtering web access correctly. This has been corrected. Note that you must add keywords to the top of the file under "keywords:" before any other filtering type, such as "urls:". See the Firewall chapter in the Software Reference for your router or switch for more information about creating these files.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00024044	Test	2	The router or switch could become unresponsive, or reboot, during a full interface test on all interfaces that lasted for a period of over 40 minutes. This only occurred when ethernet crossover cables were used as loop back cables for the interface tests. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00024282	OSPF	2	In some uncommon network configurations, it was possible that some summary LSAs may not have been propagated to all areas in the AS. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00024305	Switching	2	Previously on a 9924T switch, if you tried to create a new hardware filter when the filter database was full, the database could become corrupted until the next reboot. As well, deleting filters while the database was corrupted could result in the wrong filters being removed. This issue has been resolved. Now, if the maximum number of hardware filters is reached, any attempt to add new hardware filters will not affect the hardware filter database.	–	–	–	–	–	–	–	–	–	Y	–
CR00024695	OSPF	2	When flushing a very large amount of LSAs (4000 or more), the OSPF network neighbour relationship would become unstable, as the router or switch was not transmitting and receiving OSPF hello messages efficiently. This issue has been resolved. The ability of the router or switch to handle OSPF traffic has increased significantly.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00024758	PRI	2	The router could reset PRI interfaces more often than was necessary in the presence of line noise. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00024840	ADSL	2	Previously, line degradation on an ADSL2 or ADSL2+ connection would cause failures in the link as the router attempted to adapt to the changes in the line condition. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–
CR00025019	SFP	2	Previously, an x900-48FS switch would not recognise an inserted Coretek SFP after a restart. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00025177	OSPF	2	Previously, when multihomed links were used between OSPF neighbours and all were active (that is, the secondary links were not added with passive=on), then it was possible that the show opsf neighbour command would not display some neighbours. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00025186	PPP	2	If a router or switch was configured for both PPPoE client and Access Concentrator modes, then after a restart when the router or switch received a PPP LC Echo Request for a session that no longer existed (due to the restart) it would send an invalid PADT for that session. As a result the session would take much longer to be removed by the peer and a new session would not be established as quickly as possible. This issue has been resolved. After a restart, the router or switch will ensure that a valid PADT is sent and re-establishment of the PPPoE session happens as quickly as possible.	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y

Level 3

No level 3 issues.

Level 4

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00024786	OSPF	4	<p>Previously, when an OSPF neighbour was removed, the neighbour entry remained in the show ospf neighbour output, even after the LSA had timed out.</p> <p>This issue has been resolved. After an LSA times out for a removed neighbour, the entry is no longer shown, unless specifically requested by using the full parameter in the show ospf neighbour command.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Enhancements

No enhancements.

Features in 291-18

Software Maintenance Version 291-18 includes the resolved issues and enhancements in the following table. In the tables, for each product series:

- “Y” in a white column indicates that the resolution is available in Version 291-18 for that product series.
- “-” in a white column indicates that the issue did not apply to that product series.
- a grey-shaded column indicates that Version 291-18 was not released on that product series.
 “Y” in a grey column indicates that the issue applied to that product series. These issues are resolved in the next Version (291-19).
 “-” in a grey column indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00024484 CR00024714	Switching	2	On AT-8948 and AT-9900 series switches, the forwarding database (FDB) on the switch could lock-up when a large numbers of MAC addresses were learnt or aged on the system at a high rate (for instance, during a broadcast storm). This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00024732	EPSR	2	The switch could restart if its EPSR process requested the switch to flush its forwarding database (FDB). This could only occur on an EPSR network that contained a large numbers of VLANs and required the switch to store a large numbers of MAC addresses in its FDB. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00024760	Switching	2	Previously on AT-8948 and AT-9900 series switches, the switch could stop learning new MAC addresses during broadcast storm conditions that occurred for a long period of time. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–
CR00024889	Switching	2	MAC thrash limiting did not work in software release 291-17. This has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Levels 3 and 4

No level 3 or 4 issues.

Enhancements

No enhancements.

Features in 291-17

Software Maintenance Version 291-17 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-17 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020173	X.25	2	<p>The router or switch could restart unexpectedly when three or more X.25T circuits were all transmitting. This issue has been resolved.</p> <p>As well, the router or switch will now ensure that X.25 calls are cleared when installed in a X.25 network that sends Reset Indications in response to Reset Confirmation messages. Sometimes when an X25 network resets a circuit with a Reset Indication the network is not satisfied by a Reset Confirmation reply and continues to send a Reset Indication for every Reset Confirmation. The router or switch now counts the Reset Indications received and clears the call if more than 3 Reset Indications are received with no data transferred between them.</p>	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021338	PPP	2	Previously, PPP could unnecessarily reduce the memory available on the device for other services when configured as a PPPoE access concentrator. This occurred when a client repeatedly attempted to connect and failed (for example because of authentication failure). When the session was terminated, buffers were left allocated to the session, causing the amount of memory available to steadily reduce. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00021633	Firewall	2	When the firewall received an 500-level error from FTP, it did not always clean up the firewall sessions associated with the FTP connection. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00021772	IGMP snooping	2	Previously IGMP Snooping caused a memory leak when a host joined or left a multicast group. This was because memory allocated when the host joined the group was not returned to the memory pool when the host left the group. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00022084	Bridging	2	Previously, if a bridge filter was configured with port=none the running configuration on the router or switch would actually be set to port=all . This issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00022092	UPnP	2	Over a long period of time UPnP would exhaust the number of available TCP connections on the device and not release them. This has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00022692	Port Authentication	2	In certain network configurations, when an AR770S required authorisation from a Port Authentication device, the AR770S would fail to respond to the request packet sent from the Authenticator. This occurred only if the Authenticator was in multiple-supPLICANT mode (enabled using mode=multi in the enable portauth port command). This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00022732	PIMv4	2	<p>In normal PIM operation, assert messages are used between PIM neighbours to determine which neighbour has the better route between a multicast client and source. Once the exchange has occurred, the losing neighbour informs the winning neighbour to remove its route from the neighbour's PIM routing table. The winning neighbour forwards the multicast traffic and starts an assert timer that, when it expires, causes a new assert exchange.</p> <p>However, when the router or switch was the losing PIM neighbour, it would not correctly respond to the new assert exchange, and it would fail to tell the winning neighbour to prune its route from the neighbour's routing table. This meant that the winning neighbour would incorrectly transmit multicast traffic to the losing neighbour.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR00022932	IPsec	2	<p>Previously, the router or switch could fail to create some IPsec tunnels if the IPsec peer was specified using a DNS name (peeraddress=domainname) in the create ipsec policy or set ipsec policy commands. This occurred only when an ISAKMP policy was attached to the IPsec policy (with the isakmppolicy parameter), and the ISAKMP policy also used the peer's DNS name to identify the peer.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00022946	DHCP	2	<p>Previously, when you created a DHCP user-defined option, a null byte was attached to the end of any defined string. For example, if this option was specified:</p> <pre>add dhcp option=99 policy=name type=string value=acme</pre> <p>then when this option was included in a DHCP message, a null byte was added to "acme", making the string 5 bytes long.</p> <p>This behaviour has changed based on the option number. For options numbered between 0 and 86, the null byte is still added to the end of the string. For options numbered 87 and higher, the null byte is not added. If you override a predefined option in the range of 0 to 86 with a user-defined option, it will continue to append the string with a null byte for backwards compatibility.</p> <p>This is to meet the requirements of both RFC 2131 and 2132. RFC 2131, which defines the DHCP protocol, explicitly states that certain string fields should be null terminated (specifically options 12 and 67). This RFC and others before it have led Allied Telesis routers and switches to null terminate string-based options from 0 to 86. However, RFC 2132, which defines further DHCP and BOOTP vendor extensions, clarifies that string fields should not be null terminated.</p> <p>Note that you can use the hexstring parameter if you want to have a value that does not have the null byte appended for DHCP options between 0 and 86.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00023047	IPsec	2	Under certain IPsec policy configurations with multiple policies numbering above 24, the throughput performance of IPsec was not linear across the increasing number of policies. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00023261	STP, EPSR	2	<p>Sometimes, under sustained broadcast storm conditions and following an STP topology change or an EPSR ring state change, the switch would restart.</p> <p>This issue has been resolved.</p>	–	–	–	–	–	–	–	–	Y	Y	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023554	PRI	2	Previously, a PRI interface could lock up in the presence of line noise. This has now been fixed.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00023842	DHCP	2	Previously, on a router or switch using multihoming, the DHCP server on the router or switch could sometimes assign multiple IP address to the same client. This occurred for clients attached to an interface configured with more than one IP address. Some improvements to this issue were made in software version 2.9.1-16. This software release resolves this issue. It ensures that DHCP release, renew, and discover messages are correctly processed on interfaces with multiple IP addresses, so that the DHCP server can identify when it has already assigned a client an IP address.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00023921	RIP	2	Previously, RIP would not advertise the default route if a blackhole route had been entered into the routing table. This was caused by RIP suppressing the advertised routes based on the routes' netmask lengths instead of their preference values. This has been fixed. Please note that if your configuration relied solely on the netmask to determine if a black hole route suppressed a route advertised by RIP, you may need to have the routes' preference values adjusted so that it continues to be suppressed.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00024189	PIM	2	Previously the router or switch may have restarted if a change in unicast routing information led to a PIM Source, Group entry to no longer have an RPF interface to a source. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00024244	PPP	2	<p>The router or switch would silently discard echo-requests from a PPP peer after the peer had negotiated with it not to use the LCP magic number option. This was because the router or switch would discard echo-requests with a magic number set to 0 regardless of whether the magic number was required for the link. The magic number option is used to check that the link is not in loopback mode.</p> <p>This issue has been resolved. Echo-Requests with a magic number of 0 are now replied to if the PPP peers have negotiated not to use the LCP magic number option.</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020319	SNMP	3	<p>ASN.01 BER padding is now enabled by default. This means that SNMP adds 0x00 padding when the most significant 9 bits of an object's value are all 1. Padding enables legacy SNMP NMS systems to correctly decode this value, and provide correct readings.</p> <p>Previously the default was for the encoding to follow the ASN.01 BER rule, which cuts off the most significant byte of 0xff.</p> <p>This setting has an impact on all integer type MIB objects, including 32 bit and 64 bit counter objects.</p> <p>To remove the padding, and return to using the ASN.01 BER encoding rule, use the command:</p> <p>set snmp asnberpadding={off no false}</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Version 291-19

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020833	IP	3	When using IP NAT, TCP connections would have the sequence and/or acknowledgement numbers incorrectly altered by the router, which prevented the TCP connections from being properly set up. This issue has been fixed. Please note that NAT configured using the Firewall was unaffected by this issue.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00021128	Firewall, VRRP	3	Previously, when VRRP was configured on a router or switch that also had a Firewall NAT rule involving the same VRRP IP address, when the router or switch was in the Backup VRRP state it would reply to any incoming ARPs for the VRRP IP address with its own MAC address. This issue has been resolved. When VRRP is in the backup state, it will never reply to ARP requests for the VRRP IP address under any circumstances.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00023040	GUI, Firewall	3	When configuring LAN to WAN Firewall rules via the GUI, the “Action” drop-down box was missing the “No NAT” option. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	Y
CR00023083	IPsec	3	Previously, if the router or switch had IPsec policies create on multiple interfaces, it would sometimes fail to create a connection when it received a connection request from a valid peer. This was because the router or switch would sometimes use the wrong IPsec policy for the interface. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023393	PPP	3	<p>If the router or switch was acting as a PPPoE Access Concentrator, and it was power-cycled or restarted, then re-establishing any existing PPPoE sessions could take longer than necessary. This was because the router or switch would send the incorrect PADT in response to PPPoE session packets sent from the existing PPPoE session (EtherType of 0x8664, the PPPoE Session Protocol). Some PPPoE clients would ignore this PADT, causing a delay before the PPPoE session was re-established.</p> <p>This issue has been resolved. The router or switch now send the correct PADT in response to any existing sessions after restarting (EtherType of 0x8663, the PPPoE Discovery Protocol).</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00024495	OSPF	3	<p>Previously, if a new OSPF router ID was learned via an OSPF point-to-point (PTP) link, the original OSPF router ID was not removed from the show ospf neighbour command output.</p> <p>For PTP networks, incoming OSPF hello packets are used to update neighbour information. On an PTP interface, existing neighbours are matched by the router ID in the hello packet, whereas on other types of interfaces the neighbours are matched by source address.</p> <p>In the case of a PTP network, however, there are only ever 2 ends to the network and so there should only be one existing neighbour for the interface.</p> <p>This issue has been resolved. Now, if a new OSPF Router ID is learned via an OSPF PTP link, the original OSPF Router ID is removed from the show ospf neighbour command output.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023042	VRRP	4	<p>When a DNS query was sent to the VRRP-adopted virtual IP address on a router or switch, the relayed-response would have a source IP address of the interface it was sent from, instead of the virtual IP address.</p> <p>This issue has been fixed. DNS relay replies will now use the VRRP virtual IP address as their source address if the original query was sent to the VRRP virtual IP address.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019005	DHCP snooping	-	<p>The restriction on classifiers for DHCP snooping has been removed. This means that you can now specify a classifier number from 1 to 9999 when creating a DHCP snooping classifier. Previously, the range was restricted to classifiers numbered 1 to 100.</p> <p>The maximum number of DHCP snooping classifiers you can create has also increased to 520.</p>	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020057	DoS Attack Prevention	-	<p>The AlliedWare™ Operating System now includes a Denial of Service Attack Protection feature for AT-8600 Series switches. This enhancement allows you to configure specific defences against the following types of DoS attacks:</p> <ul style="list-style-type: none"> ■ IP Options ■ LAND Attack ■ Ping of Death Attack ■ Smurf Attack ■ SYN Flood Attack ■ Teardrop Attack <p>For more information about configuring DoS Attack Prevention, see the <i>AlliedWare™ Operating System Software Reference for Version 2.9.1 DoS Attack Prevention Edition</i> available for AT-8600 Series switches. You can download this software reference from: www.alliedtelesis.co.nz/documentation/</p>	-	-	-	-	-	-	Y	-	-	-	-
CR00020882	Firewall	-	<p>A new compatibility mode allows the firewall to interoperate with the SAMSUNG SmartViewer 2.0 for ProDVR application. This application uses RSTP over TCP to communicate with SAMSUNG IP security cameras.</p> <p>To use this application on a router or switch with a firewall configured, you must add a new application rule for RTSP to your firewall policy:</p> <p style="padding-left: 40px;">add firewall policy=[policy-name] apprule=app-rule-id action=allow interface=[interface] application=rtsp compatibility=smartviewer</p>	Y	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021615	ADSL, Core	-	<p>With this software version, AR441S routers with a hardware revision of M1-2 (or later) will support ADSL2 and ADSL2+ connections. You can see the hardware revision of a router by entering the command show system and checking the “Rev” column for the “Base” board.</p> <p>When running this software version, AR441S routers with rev M1-2:</p> <ul style="list-style-type: none"> ■ have the following new options for the command set adsl standard: <ul style="list-style-type: none"> adsl2 connect only to devices offering ADSL2 adsl2plus connect only to devices offering ADSL2+ auto2plus connect at ADSL2+ if this is offered by the other end device (CO), or otherwise automatically fall back to what is offered ■ have a default ADSL standard setting of auto2plus ■ behave as they currently do for other ADSL standard settings <p>When running this software version, existing AR441S routers with a hardware revision of M1-1 or earlier:</p> <ul style="list-style-type: none"> ■ do not have the new options adsl2, adsl2plus, or auto2plus for the command set adsl standard ■ still use the existing default ADSL standard setting of auto, which allows automatic fallback connection for ADSL standards only. 	Y	-	-	-	-	-	-	-	-	-	-
CR00023867	Switching	-	The maximum number of uplink ports available for private VLANs has increased from 50 to 150.	-	-	-	Y	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023990	PPP	-	<p>Two new parameters, ipfilter and ipfragment, are now available for the create ppp template and set ppp template commands:</p> <pre>create ppp template=ppp-template [ipfilter=NONE[0..999] [ipfragment=ON OFF True False Yes No] set ppp template=ppp-template [ipfilter=NONE[0..999] [ipfragment=ON OFF True False Yes No]</pre> <p>These parameters are useful when a dynamic IP interface is created over the dynamic PPP interface. The shortest valid strings are ipfi for ipfilter and ipfr for ipfragment.</p> <p>The ipfilter parameter specifies the traffic filter to apply to IP packets transmitted or received over the dynamic IP interface. The filter must already have been defined with the add ip filter command. The dynamic IP interface may have a maximum of one traffic filter but the same traffic filter can be assigned to more than one interface. Traffic filters are applied to packets received via the dynamic IP interface. The default is to not apply a filter.</p> <p>The ipfragment parameter specifies whether the “Do not fragment” bit is obeyed for outgoing IP packets that are larger than the MTU of the interface. If yes, the “Do not fragment” bit is ignored and outgoing IP packets larger than the MTU of the interface are fragmented. This is particularly useful for interfaces configured with GRE, SA, or IPsec encapsulation, which can potentially increase packet sizes beyond the MTU of the interface. If no, the “Do not fragment” bit is obeyed and IP packets larger than the MTU are discarded. This is normal behaviour for IP. The fragment parameter has no effect on packets smaller than the interface MTU. The default is no.</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Features in 291-16

Software Maintenance Version 291-16 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-16 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00017581	Firewall	2	Sometimes in congested networks, when processing certain out-of-order FTP or RSTP TCP packets the firewall could leak some memory. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	Y
CR00019431	Bridge, L2TP, PPP	2	With some L2TP/PPP configurations, disabling the port or removing the cable from the port caused the router to reboot. Improvements related to this issue were made in software version 291-12. This version contains further improvements to prevent the issue occurring.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00020257	ATM	2	With M3 versions of the AR441S, sometimes when the router was restarted the ADSL link would come up, but packets larger than two cells would often be received with CRC errors and discarded. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020937	QoS	2	Under some configurations, the switch could reboot when: <ul style="list-style-type: none"> ■ applying a QoS policy to the same port twice (by using the command set qos port=x policy=x). ■ adding classifiers to a QoS flowgroup that has not been associated with a policy or traffic classifier. These issues have been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00021623	Switching	2	Previously when a MAC learning limit was enabled along with MAC re-learning for a switch port, if the same MAC addresses were learnt by another port in the same vlan (a 'station move' event), the learn limit on the first port was not decremented even though the MAC addresses were no longer tied to it. This would mean that after the port reached its learn limit, it would stop learning any new MAC addresses even if all of the previously learnt addresses were then moved to different ports. This issue has been resolved. Now when a MAC address undergoes a 'station move' event, the learn counter of the first switch port will be decremented when the MAC is removed, so the port can no longer get into a state where it will refuse to learn more MAC addresses.	-	-	-	-	-	-	-	-	Y	Y	-
CR00021993	EPSR	2	Previously when an EPSR+ ring was recovering from multiple link failure, IP connectivity could be lost for longer than necessary. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00022057	IPv6	2	Previously, if a router or switch received a neighbour discovery advertisement with a target link-layer address option of 00-00-00-00-00-00, the device may have restarted. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00022153	DHCP	2	Previously, on a router or switch using multihoming, the DHCP server on the router or switch could sometimes assign multiple IP address to the same client. This occurred when a client's DHCP Discover message was received through more than one logical interface on the router or switch. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00022292	Switching	2	On some occasions, inserting an Allied Telesis AT-G8T copper GBIC stopped the GBIC ports from operating correctly. The GBIC LEDs would also display the wrong state (lit when the GBIC was removed or off when the GBIC was inserted). This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-	Y
CR00022437	IPsec, L2TP	2	Previously some specific network configurations would not work when L2TP was secured with IPsec transport mode through NAT. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00022482	LLDP	2	Previously a downstream device could learn the router or switch's MAC address when it received an LLDP DU. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00022545	L2TP	2	Previously, when a router or switch at one end of an L2TP tunnel rebooted, it would have to wait for the tunnel on the other end to timeout before it could recreate the tunnel. This caused a delay in recreating the tunnels after a restart. This issue has been resolved. Also, under some situations, when an L2TP tunnel was destroyed the router or switch would crash. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00022596	Port Authentication	2	Previously on an AR-770s, the command: enable portauth=8021x port= <i>portid</i> type=authenticator guestvlan= <i>vlanid</i> would not add the specified port to the specified guest VLAN if executed from the device boot configuration script. This issue has been resolved.	-	-	Y	-	-	-	-	-	-	-	-
CR00022647	BOOTP	2	Previously if a router or switch acting as a BOOTP relay had two subnets, and one was a super net of the other, the router or switch could forward DHCP messages with the broadcast flag set to the wrong interface. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00022985	L2TP	2	Previously, under some heavy load traffic conditions, L2TP tunnels would experience a periodic latency or sometimes no longer function. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00022993	PIMv4	2	Previously on specific network configurations, using PIM Sparse Mode could cause a memory leak. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
CR00023012	IP	2	A security vulnerability was found in the design of the DNS protocol. This vulnerability has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00023053	BGP	2	A security vulnerability was found in the implementation of BGP. This vulnerability has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00023082	RADIUS	2	RADIUS servers can specify multiple dynamic routes to a user, in addition to the normal host specific route to the allocated address. These additional routes are called framed-routes in RADIUS configuration definition. Previously, the maximum number of framed-routes that could be created by the RADIUS server on the router or switch were limited to 2 per client. This limit has increased to 32 routes.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00023347	L2TP, IPsec	2	<p>Previously, the router or switch could reboot while a L2TP tunnel was being established over an IPsec connection. This occurred only when the device received either:</p> <ul style="list-style-type: none"> ■ a request to establish a secure channel from a source that does not match an IPsec policy, or ■ a L2TP call disconnection notification (CDN) or a Stop Connection (StopCCN) with values outside of those specified by the L2TP RFC. <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	–

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021620	STP	3	Previously the set mstp cist port command parameters intpathcost and extpathcost could not have the value default set. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
CR00021821	IPsec	3	In certain situations on an IPsec network, queued packets were not discarded despite reaching their retry timeout period. While a router or switch is establishing a Security Authorisation with its peer, it keeps a queue of the packets waiting to be sent across the network. These packets have a retry timeout period and if this period is reached, the packets should be discarded. This issue has been resolved. Packets that reach their retry period are now discarded from the queue.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00022301	Bridging	3	Previously if ATM was used as the WAN interface in a remote bridge and the bridge had more than 1 VLAN, then the VLAN module would drop the bridged frames. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–
CR00023011	LT2P, Firewall	3	Previously, the firewall on the router or switch would block some L2TP control messages during a route change (for example, when a PPP connection was coming up). This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

Level 4

No level 4 issues.

Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019706	PPP	-	<p>A new parameter ipborrow has been added to the create and set ppp interface commands. You can set the ipborrow parameter to the values: yes on true no off false.</p> <p>This parameter is required in the following situation: the PPP interface has been configured as an unnumbered IP interface (i.e. configured with IP address 0.0.0.0), but you do not want the PPP peer to allocate an IP address to be used on the local PPP interface (i.e. iprequest=no). In this case, the router or switch needs to present a non-zero IP address to the peer during IPCP negotiation. The solution to this problem is to use another IP address that has been configured on the router or switch (invariably another interface on the device will have been configured with a non-zero IP address). With the ipborrow parameter, you can configure the unnumbered PPP interface to 'borrow' this other interface's IP address to use as the IP address it presents to the peer during IPCP negotiation.</p> <p>If there are multiple non-zero IP interfaces on the router or switch, you cannot specify which interface's IP address the unnumbered PPP will borrow; it will simply borrow the IP address from the interface with the lowest ifindex.</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00021106	IPsec, ISAKMP	-	You can now specify peers in ISAKMP and IPsec policies using a DNS name. Previously, you could only specify the peers using an IP address.	Y	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021262	IPsec	-	<p>This enhancement has improved router or switch performance when:</p> <ul style="list-style-type: none"> ■ multiple IPsec policies exist. In particular, having two policies causes much less of a reduction in performance. ■ a single channel exists with bidirectional traffic (i.e. the single channel is both encoding and decoding packets). <p>Some improvements for this situation were made in 291-15. This version contains further improvements.</p>	Y	Y	Y	Y	-	Y	-	-	-	-	-
CR00021769	SNMP	-	<p>A new command set snmp trapdelay has been added to allow SNMP traps to be queued for a specified time at start up.</p> <p>By default, all SNMP traps are queued for 10 seconds following startup. This allows time for links to come up on the router or switch. However sometimes this is not enough time for other network protocols to converge and open up transmission paths to the SNMP management station.</p> <p>The set snmp trapdelay command allows you configure a longer delay of up to 10 minutes on an SNMP trap. To change the delay, use the command:</p> <p>SET SNMP TRapdelay=10..600</p> <p>The default is 10 seconds.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00021852	EPSR	-	<p>An enhancement has been made to EPSR to speed up recovery time in situations where the Master switch is isolated or down. In these situations, if any links between transit nodes go down and are restored, the transit nodes are now able to put the recovered ports back into a forwarding state even without messaging from the Master switch. This means that connectivity around the ring can be partially restored before communication with the Master has been restored.</p> <p>The mechanism by which the transit nodes make this decision operates in a way that prevents the possibility of the ring ever becoming unprotected.</p>	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00022331	SHDSL	-	Previously on AR442S routers, SHDSL train up times were variable and frequently longer than one minute. This enhancement reduces this variability and minimises the train up time required.	Y	-	-	-	-	-	-	-	-	-	-
CR00022832	SNMP	-	<p>The set interface command now has the parameter trapdelay, which allows you to delay the transmission of SNMP link status traps from 0 to 60 seconds. This is useful for situations where the SNMP link status traps need to wait for route tables to be updated or other protocols to process the link change event before being transmitted. The new command is:</p> <pre>set Interface={ifIndex}interface trapdelay=0..60</pre> <p>Note that you cannot set a delay on a dynamic interface. The default is 0.</p> <p>The output of the show interface=interface command now displays the value for this parameter.</p> <p>Note that this changes the behaviour set by CR00021581 in software version 2.9.1-15, which introduced a fixed 5 second delay for link status traps.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Features in 291-15

Software Maintenance Version 291-15 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-15 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020914	DVMRP	2	When using DVMRP for multicast traffic, if the router or switch received a leave request from the last remaining client in a multicast group before it could fully establish the DVMRP session for that group, the router or switch would not send a prune message to the upstream router and would continue to receive multicast traffic for that group. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00021146	EPSR	2	Previously, it was possible for non-EPSR messages such as IGMP snooping query solicitation messages to be sent on the EPSR control VLAN if the control VLAN was part of an STP topology. Since the control VLAN is designed as an intentional loop so that the master node can monitor the integrity of the loop, other messages on the control VLAN can form a packet storm. This issue has been resolved. All switches in an EPSR ring now discard all non-EPSR messages on the control VLAN.	–	–	–	–	–	–	–	–	Y	Y	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021342	BGP	2	A small memory leak was occurring when receiving BGP update messages. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00021491	DVMRP	2	When DVMRP had pruned an incoming multicast stream, if that stream continued to be transmitted and pruned correctly, after 24 hours the downstream DVMRP neighbour could stop successfully pruning that stream. At this point the downstream neighbour would be receiving the traffic on the interface even though it had no downstream receivers. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00020593	Firewall	2	When using multiple firewall policies, TCP connections created across the policies would have any TCP options (such as timestamps or window scaling) stripped out of the SYN packets. This could cause slow downs or other problems for programs that rely on those TCP options being present. This has been resolved—the TCP options will no longer be stripped from the SYN packets in this case. Also, the RFC1323 TCP window scaling option, if present, would not be correctly applied to FTP data connections (FTP connections on port 20), resulting in low throughput for FTP file transfers. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	Y
CR00020643	Flash file system	2	An error in the flash file rename code could occasionally result in flash file system header corruption, leading to flash file system inconsistencies. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00020677	IPsec	2	Previously, one of the memory buffers displayed in output of the command show buffer scan was periodically increasing, because of an IPsec issue. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR00020700	WAN load balancing	2	Previously, AR750S and AR770S routers required a special feature license for WAN load balancer. This issue has been resolved. A license is no longer required for these routers.	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021006	Switching	2	When ingress filtering was enabled on a port and a packet arrived on that port with a VLAN identifier that the port was not a member of, the source MAC address would be incorrectly learnt. This issue has been resolved and in this situation the MAC address is no longer added to the forwarding database.	-	-	-	-	-	-	-	-	Y	Y	-
CR00021259	Switching, VLAN	2	If a VLAN-tagged ARP request was received with a VLAN ID of a VLAN that had previously existed but had been destroyed, the switch could reboot. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00021308	OSPF	2	In a configuration where two otherwise identical external OSPF routes had been learnt to a particular destination over two different interfaces, when one of the interfaces went down both routes would be permanently removed from the routing table and would not be added until OSPF was reset. This issue has been resolved. Only the route belonging to the downed interface will be removed.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00021978	Switching	2	If an ARP was received on a port and the MAC associated with that ARP subsequently moved to another port and had a new IP associated with it, and the new port was on a different switch instance, then when the original ARP timed out, the MAC would be removed from the switch's forwarding database. This only happened if the ARP moved across switch instances. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020551	DHCP	3	Previously, when an AT-8600 series switch was acting as a DHCP server with a range defined, frequent Flash memory compactions would occur. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–
CR00020710	Switching	3	The show switch fdb port=<number> command was displaying FDB information on incorrect ports. This issue has been resolved. Also, if the show switch fdb port=<number> command is run where the port specified is in a trunk, all FDB entries for that trunk will be displayed, irrespective of which actual port the source MAC ingressed.	–	–	–	–	–	–	–	–	Y	Y	–
CR00020794	Switching	3	If a user set a description on an AT-9924 switch port and then used the command show int counter or show int=<id> to display interface counters, the command output would include counters called ifInDiscards and ifOutDiscards. However, these counters do not apply to these switches. This issue has been resolved, so these counters no longer display.	–	–	–	–	–	–	–	–	–	Y	–
CR00020795	Switching	3	Previously, conditions existed where it was possible to remove a GBIC from a AT-8800 or AT-8600 series switch, but have the GBIC LED stay on. This could occur if a GBIC had been inserted into the switch in such a way that the GBIC pins did not all make electrical connection at the same time. This issue has been resolved. Removing a GBIC now always results in the LED being turned off.	–	–	–	–	–	Y	Y	–	–	–	–
CR00021265	IP gateway	3	If the traceroute command was used from a Windows-based device to trace the path to a destination through a switch which had two potential return paths, then the traceroute command did not always produce the correct results. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021267	Bridging	3	If the router received a CDP packet, and CDP was disabled (the default state), and bridging was configured, then the packet would not be bridged. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00021581	SNMP	3	Previously, the switch did not always successfully transmit SNMP link status traps. This issue has been resolved. SNMP link status traps are now delayed for 5 seconds to allow lower layer interfaces to come up.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021766	Switching	4	If a port was set as a loopback on an AT-8948 or x900-48FE series switch, and was configured with a speed of 10mhauto , the LEDs did not display correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–

Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00018895	SSH	-	Secure Shell (SSH) no longer requires a feature licence. SSH server and client functionality now works when no feature licence is present.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00020566 CR00021186	EPSR	-	<p>This software version includes support for EPSR+ with enhanced multiple link recovery. This enhancement enables an EPSR ring to recover from simultaneous failure of multiple links or units, no matter where in the ring these failures occur.</p> <p>With enhanced recovery, if a ring has multiple points of failure, and then one point recovers, the recovered point will start processing traffic even if other points are still down. This keeps as much of the ring available as possible.</p> <p>To enable enhanced recovery, use one of the commands:</p> <pre>create epsr=<id> enhance=on set epsr=<id> enhance=on</pre> <p>Note that you must enable enhanced recovery on the master node and every transit node within the EPSR domain.</p> <p>Enhanced recovery is disabled by default, to allow interoperability with other implementations that are based on RFC 3619.</p> <p>To disable enhanced recovery, use one of the commands:</p> <pre>create epsr=<id> enhance=off set epsr=<id> enhance=off</pre> <p>To see whether it is enabled or disabled, use the command:</p> <pre>show epsr</pre> <p>and check the "Enhanced Recovery" field.</p>	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800																				
CR00021061	NSM	-	<p>This software version includes support for new variants of the Rapier 24i and Rapier 48w switches, which have new NSM bay connectors. You can identify the new switch variants by the following board IDs:</p> <table><tr><th>Board ID</th><th>Name (as displayed by show system)</th></tr><tr><td>-----</td><td>-----</td></tr><tr><td>311</td><td>AT-RP24i-B Rapier 24i NEBS</td></tr><tr><td>312</td><td>AT-RP24i-B Rapier 24i DC NEBS</td></tr><tr><td>302</td><td>AT-RP48w-B-15 Rapier 48w-AC</td></tr><tr><td>300</td><td>AT-RP48w-B-85 Rapier 48w</td></tr></table> <p>The new connectors are compatible with the following new NSM variants:</p> <table><tr><th>Board ID</th><th>Name</th></tr><tr><td>-----</td><td>-----</td></tr><tr><td>313</td><td>AT-AR040-B-00 NSM 4PIC</td></tr><tr><td>314</td><td>AT-AR048-B NSM DS3</td></tr></table> <p>Only the new switch variants can use the new NSMs. Other Rapier 24i and Rapier 48w switches continue to use the original NSMs (which have board IDs of 87 and 187).</p>	Board ID	Name (as displayed by show system)	-----	-----	311	AT-RP24i-B Rapier 24i NEBS	312	AT-RP24i-B Rapier 24i DC NEBS	302	AT-RP48w-B-15 Rapier 48w-AC	300	AT-RP48w-B-85 Rapier 48w	Board ID	Name	-----	-----	313	AT-AR040-B-00 NSM 4PIC	314	AT-AR048-B NSM DS3	-	-	-	Y	Y	-	-	-	-	-	-
Board ID	Name (as displayed by show system)																																	
-----	-----																																	
311	AT-RP24i-B Rapier 24i NEBS																																	
312	AT-RP24i-B Rapier 24i DC NEBS																																	
302	AT-RP48w-B-15 Rapier 48w-AC																																	
300	AT-RP48w-B-85 Rapier 48w																																	
Board ID	Name																																	
-----	-----																																	
313	AT-AR040-B-00 NSM 4PIC																																	
314	AT-AR048-B NSM DS3																																	
CR00021262	IPsec	-	<p>This enhancement has improved router or switch performance when:</p> <ul style="list-style-type: none">■ multiple IPsec policies exist. In particular, having two policies causes much less of a reduction in performance.■ a single channel exists with bidirectional traffic (i.e. the single channel is both encoding and decoding packets).	Y	Y	Y	Y	-	Y	-	-	-	-	-																				

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021304	IPsec	-	<p>Changes have been made to reduce the risk of packet loss over a VPN under very high traffic levels and corresponding high-to-overload CPU conditions.</p> <ul style="list-style-type: none"> ■ The number of input buffers allowed for IPsec message processing has been increased, to mitigate brief (<50ms) periods of CPU overload where the arrival of IPsec packets can exceed the router or switch's ability to process them in real time. This prevents packet loss. ■ Processing of the ISAKMP heartbeat between two peer routers or switches has been given the highest priority over packet stream encryption, to ensure that the security authorisation synchronisation is not lost during high traffic rates. Loss of synchronisation results in packet loss until a resynchronisation completes. 	Y	Y	Y	Y	-	Y	-	-	-	-	-
CR00021752	SHDSL, GUI	-	<p>It is now possible to use the web-based GUI to display SHDSL counters and statistics on AR442S routers. The new pages are available from the left-hand menu under:</p> <p>Diagnostics > Layer 1 Counters > SHDSL Counters</p> <p>Diagnostics > SHDSL Statistics.</p>	Y	-	-	-	-	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021896	VLAN	-	<p>This enhancement enables administrative (virtual) activation of VLANs. When a VLAN is activated virtually, its IP interface is active (and therefore usable) even if all its ports are physically disconnected. The IP interface associated with the virtually activated VLAN can be operated by protocols such as OSPF, BGP, and RIP.</p> <p>VLAN activation is useful for VLANs that are reached through L2TP tunnels instead of through switch ports.</p> <p>To turn virtual activation on or off, use the command:</p> <pre>SET VLAN={vlan-name 1..4094 ALL} VIRTActivation ={Yes No}</pre> <p>The default is no.</p> <p>To see whether the VLAN has been activated virtually, use the command show vlan and check the new "Admin Active" field.</p> <p>This enhancement was previously only available on Rapier, AT-8800, AT-8600 and AT-8700XL switches. Now it is available on all devices that support VLANs.</p>	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y

Features in 291-14

Software Maintenance Version 291-14 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” in a white column indicates that the resolution is available in Version 291-14 for that product series.
- “-” in a white column indicates that the issue did not apply to that product series.
- a grey-shaded column indicates that Version 291-14 was not released on that product series.
 “-” in a grey column indicates that the issue did not apply to that product series.
 “Y” in a grey column indicates that the issue applied to that product series. These issues are resolved in the next Version (291-15).

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019178	VRRP	2	When using monitored interfaces in conjunction with VRRP, if a primary master device was brought into the backup state by the monitored interface going down, it would continue to reply to ARP requests for the virtual IP address with its own MAC address. This issue has been resolved. The device will now ignore ARP requests in this situation.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020266	Switching	2	If a network event caused the switch to flush its layer 2 forwarding database (FDB) for a port, in some circumstances the switch also flushed hardware ARP entries that hardware layer 3 routes were still using. Possible triggers included an STP topology change somewhere else in the network, or a link flap on a port. Depending on the network configuration and/or network traffic, this issue could result in incorrectly layer 3 switched traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–
CR00020413	DHCP snooping, IGMP snooping	2	<p>IGMP snooping did not correctly snoop IGMP traffic that arrived on an untrusted DHCP snooping port.</p> <p>This issue has been resolved. IGMP packets are processed now, unless IP filtering is enabled in DHCP snooping. Note that IP filtering is enabled by default, so the switch will drop IGMP packets by default if DHCP snooping does not have the source host as a current valid entry in the DHCP snooping database.</p> <p>To disable or enable IP filtering in DHCP snooping, use the commands:</p> <p style="padding-left: 40px;">disable dhcpsnooping ipfiltering</p> <p style="padding-left: 40px;">enable dhcpsnooping ipfiltering</p> <p>DHCP snooping must be enabled for IP filtering to take affect, but IP filtering cannot be disabled or enabled while DHCP snooping is enabled.</p>	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
CR00020759	Switching	2	On AT-8948 switches running version 291-13, SFPs did not work—the link did not come up. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00015046	L2TP	3	When the L2TP speed was changed, output of the command show ppp util still showed the old speed. This issue has been resolved. The previous behaviour was not incorrect, because the new speed only takes effect when the L2TP tunnel is restarted by deactivating and reactivating the call. The router or switch now displays a message to indicate this.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00019267	Hotswapping	3	Occasionally, AT-8948 and x900-48 series switches rebooted or gave an invalid error message when hotswapping a PSU or FOM unit in. The invalid error message was about an airflow direction mismatch. The PSU or FOM would function correctly, but the switch would display incorrect information in output of the show system command. This issue has been resolved so that the switch does not reboot. If the error occurs, the switch displays a console message to indicate that a failure occurred when hotswapping in, and a log message will record the failure. If there was a failure when hotswapping the PSU or FOM in, the switch will display a console message when the PSU or FOM is swapped out.	–	–	–	–	–	–	–	–	Y	–	–
CR00020168	L2TP	3	If the router or switch attempted to establish an L2TP tunnel over a link that was down, multiple tunnels were created when the link was re-established. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Level 4

No level 4 issues.

Enhancements

No enhancements.

Features in 291-13

Software Maintenance Version 291-13 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-13 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00018575	L2TP	2	If an L2TP tunnel had a large number of PPP interfaces over it, and the link that the L2TP tunnel was over went down, the router or switch might restart. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00019285	SHDSL	2	The AR442S router's SHDSL interface would not "train up" with some Alcatel DSLAMs, because of an EOC message exchange issue. This issue has been resolved. Some other issues with EOC message reception were also resolved.	Y	–	–	–	–	–	–	–	–	–	–
CR00020240	PIM	2	In PIM, if the RPF neighbour to the source or the RP changed as a result of a unicast route change, and there were slow route updates, and that meant a new route to the RPF could not be found within 5 seconds, then multicast traffic would not resume correctly once the new routing information was learned. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020253	IP gateway	2	If multicast traffic was being forwarded to a PPP interface and that PPP interface went down, the router or switch would restart. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00020436	DHCP snooping	2	DHCP Snooping did not correctly block traffic from untrusted IP addresses, because it did not correctly create the required filters. This issue has been resolved. Note that this issue did not apply on x900-48, AT-8948, or AT-9900 series switches, because you create the filters manually on those switches.	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00020522	DHCP snooping	2	If a client sent an ARP request to a DHCP Snooping switch, the DHCP Snooping switch would drop the ARP packet at its CPU. This issue has been resolved. Note that this issue did not apply on x900-48, AT-8948, or AT-9900 series switches.	–	–	–	Y	Y	Y	Y	Y	–	–	–

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00010538	Firewall	3	<p>When firewall events were recorded in the Notify queue (displayed in output of the command show firewall event=notify), the IP address shown would be the address of the very first packet that belonged to that event flow. For example, if 64 host scan packets were required to trigger a host scan event and the first packet had a target IP of 1.1.1.1 and the 64th had an IP of 1.1.1.64, then the IP address recorded would be 1.1.1.1, even though the event was not actually recorded until the 64th packet arrived. Additionally, the source and destination ports in this display would always show as 0.</p> <p>These issues have been resolved. The IP addresses shown are now those of the particular packet that triggered the event notification, and the source and destination ports match the actual ports used by that packet.</p> <p>These issues were partially resolved in an earlier version—this version contains an improved resolution.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00019207	Switching	3	<p>A small number of x900-48 series switches were experiencing link problems for some ports with some SFPs.</p> <p>This issue has been resolved.</p>	–	–	–	–	–	–	–	–	Y	–	–
CR00020023	RSTP, SNMP	3	<p>If the STP state of a switch port in a Rapid Spanning Tree was monitored via SNMP using the BRIDGE-MIB, the value reported for a port in the Alternate role was Listening when it should have been Blocking. Similarly, Blocking was reported for a port in the Disabled role when it should have been Disabled.</p> <p>This issue has been resolved.</p>	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00020243	SNMP, IP gateway	3	<p>Previously, the router or switch would respond to SNMP requests destined for broadcast addresses.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020320	IPsec, IP gateway	3	In some configurations using PPPoE and IPsec, inappropriate ICMP redirect messages would be generated. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR00020354	Switching	3	AT-8848 switches would drop DHCP packets if they ingressed at a port on one switch instance and should have egressed out a port in the other switch instance. Ports 1 to 24 and the uplink port 50 are on instance 0. Ports 25 to 48 and the uplink port 49 are on instance 1. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–
CR00020376	SNMP, IGMP	3	SNMP could not always access all the group members in the IGMP interface group table. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

No level 4 issues.

Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00017819	MACFF	-	MAC-forced forwarding static server entries and debugging has been improved. For details, see "MAC-forced forwarding enhancements (CR00017819)" on page 161 .	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00019547	VLAN	-	<p>This enhancement enables administrative (virtual) activation of VLANs. When a VLAN is activated virtually, its IP interface is active (and therefore usable) even if all its ports are physically disconnected. The IP interface associated with the virtually activated VLAN can be operated by protocols such as OSPF, BGP, and RIP.</p> <p>VLAN activation is useful for VLANs that are reached through L2TP tunnels instead of through switch ports.</p> <p>To turn virtual activation on or off, use the command:</p> <pre>SET VLAN={vlan-name 1..4094 ALL} VIRTActivation ={Yes No}</pre> <p>The default is no.</p> <p>To see whether the VLAN has been activated virtually, use the command show vlan and check the new "Admin Active" field.</p>	-	-	-	Y	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020309 CR00020326	BRI	-	<p>This release adds support for the V3 hardware revision of the AT-AR021 BRI-S/T Port Interface Card (PIC). The AT-AR021 V3 hardware revision is a plug-in replacement for the V2 hardware revision, which is no longer available. The AR021v3 has the same feature set and command set as the AR021v2, except that it does not support NT mode operation. Existing configurations for normal TE mode operation will run unchanged on the AR021v3.</p> <p>The AR021v3 PIC can be installed in the following expansion bays:</p> <ul style="list-style-type: none"> ■ PIC bays on the AR415S, AR440S, AR441S, AR442S, AR725, AR745, AR750S, AR750S-DP, and AR770S routers ■ AT-AR040 NSM installed in the AR745 router, Rapier 16fi, Rapier 24i, and Rapier 48w switches. 	Y	Y	Y	Y	Y	-	-	-	-	-	-
CR00020370	Switching	-	Support for the RoHS-compliant AT-G8T GBIC was added for AT-9800 series switches. Before this, the GBIC would fail to link up with the slide switch set to auto (its default position).	-	-	-	-	-	-	-	-	-	-	Y

Features in 291-12

Software Maintenance Version 291-12 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-12 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues.

Level 2

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019066	L2TP	2	Under certain conditions, entering the show l2tp tun call command would cause the router or switch to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00019431	Bridge, L2TP, PPP	2	With some L2TP/PPP configurations, disabling the port or removing the cable from the port caused the router to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00019923	LACP, VLAN	2	The switch sometimes rebooted if a port was added to a private or nested VLAN when LACP was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–
CR00020051	Switching	2	If trunked ports were quickly removed from a device (for example, by powering off the device that the trunked ports were connected to), it was possible for the trunk’s master port to become a port that was not a member of the trunk. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–

Level 3

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00018949	Core	3	<p>When a PSU or FOM was hotswapped and replaced with a new unit of the same type, the switch did not update the serial number of the hotswapped unit. Output of the commands show system and show log displayed the serial number of the previous unit.</p> <p>The same issue occurred with PICs in NSM units. For example, if you hot swapped out an NSM with a BRI PIC and then replaced that PIC with another identical PIC, and then hot swapped the NSM back into the bay, the new PIC's serial number was not displayed.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	–	–	–	Y	Y	–
CR00019557	IPsec	3	<p>Previously, if the router was trying to establish a VPN and the peer sent a proposal that had more than 4 transforms in it, the router did not establish the VPN, and could reboot.</p> <p>In IPsec, each transform specifies a possible set of security parameters for the proposed tunnel. You can see the number of transforms in a VPN proposal by entering the command enable isakmp debug, attempting to establish the tunnel, and looking for messages with text like:</p> <pre>Proposal#: 1 Protocol: ESP(3) #Trans: 8 SPI: 9624fe10 Transform#: 1 ...</pre> <p>This issue has been resolved. The router now accepts and can send proposals with up to 10 transforms, although it is unusual to need more than 4. Also, if the router receives a proposal with too many transforms, it sends an error message in response instead of rebooting.</p>	Y	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019870	Firewall	3	The firewall's TCP Setup Proxy did not always calculate the MSS value correctly. Instead, it would sometimes set the MSS value to 536 bytes, regardless of the MSS value in the incoming SYN packet. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	Y
CR00020045	SNMP	3	When using an SNMP browser to manager the Rapier 16fi, a user may have seen an incorrect System Identity reported for variants with MT-RJ fibre ports. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–
CR00005048	GUI	3	When using the web-based GUI to add an IP Interface to a PPP connection, not all the available PPP instances were selectable. This issue has been resolved. Additionally, you can now use the GUI to give an ethernet interface a DHCP-assigned IP address, and to enable or disable the IP request option for PPP dynamic assignment.	Y	–	Y	–	–	–	–	–	–	–	–

Level 4

No level 4 issues.

Enhancements

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00018418	IGMP, MIB	-	AlliedWare now includes an IGMP Group MIB. This MIB is available in the file at-igmp.mib. It has the object identifier prefix igmp ({ modules 139 }), and contains a collection of objects and traps for monitoring IGMP group membership. For more information, see “IGMP Group MIB (CR00018418)” on page 162 .	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00019548	PRI	-	With this enhancement, the show pri state command now displays any current loopback configuration and lists any running tests on PRI ports.	Y	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00019989	Switching	-	<p>A new command has been added to modify the operation of the switch when a packet uses the default hardware multicast route. This usually happens when the switch receives new unregistered multicast traffic. The command syntax is:</p> <pre>SET SWItch DEFaultmrouteoperation={TRap ROUte DEFault}</pre> <p>The defaultmrouteoperation parameter specifies the operation to perform on the first packet received for a multicast stream. If you specify trap or default, the packet is copied to the CPU for processing, and is also flooded to other ports in the VLAN. Under some circumstances, especially when an L3 multicast routing protocol such as PIM is configured, the packet may not be flooded correctly to other ports on the receiving upstream VLAN. If you specify route, the packet is copied to the CPU and also routed on the receiving upstream VLAN. In some circumstances this may change the packet's VLAN tag. The default is trap.</p> <p>Important: Setting this command to route changes the default behaviour of the switch hardware, may change the VLAN tag, and may cause issues in private VLAN configurations. We recommend that you only change this setting if clients on the receiving VLAN are not receiving the first packet of a new multicast stream and this is affecting the multicast service.</p> <p>To see the current setting, use the command show switch and check the entry called "Def. Multicast Route Op".</p>	-	-	-	-	-	-	-	-	Y	Y	-
CR00020024	Bridging	-	In Software Version 291-11, CR00019152 increased the maximum number of bridge ports supported, but with the trade-off of reduced bridging performance for small packets. This CR completes the enhancement by restoring bridging performance to its earlier level.	Y	Y	Y	Y	Y	-	-	-	-	-	-
CR00020146	IP gateway	-	The upper limit on the number of entries in an IP filter has been increased from 255 to 3072.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x / AR450	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00020171	Eth	-	<p>Log entries are now generated when Ethernet port links are taken up or down. Typical log entries are:</p> <p>26 11:37:18 6 ETH PINT DOWN ETH3: interface is DOWN</p> <p>26 11:37:28 6 ETH PINT UP ETH3: interface is UP</p> <p>Note that AR022 PICs (ETH PICs) do not enter a log message after a restart if the link is up during that restart, but do enter a log message for each subsequent link transition.</p>	Y	Y	Y	-	-	-	-	-	-	-	-

Features in 291-11

Software Maintenance Version 291-11 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version Version 291-19 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00000704	PPP, SYN	2	Previously when a SYN link failed and the link indication signal (e.g. Carrier Detect) was de-asserted, then output of show interface would show the SYN interface as down, but the PPP interface would remain up until PPP Link Quality Reporting (LQR) determined that the link was no longer operational. Depending on the LQR timer setting, this could take many seconds. This issue has been resolved. The PPP link now goes down within a few seconds of the SYN link going down.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00007153	DHCPv6, IPv6, PIMv6, Software QoS	2	Previously, it was only possible to create 2048 IPv6 interfaces on switches with IPv6 support in hardware (x900-48 series switches and AT-8948 switches with an accelerator card installed). This issue has been resolved. You can now create up to 4096 IPv6 interfaces on these switches.	–	–	–	–	–	–	–	–	Y	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007412	PIM, PIMv6	2	PIM Null-Register packets were being generated with incorrectly formatted dummy multicast data. This issue has been resolved, so that the packets conform to the formats specified in RFC 4601, Section 4.9.3. Register Message Format.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR00008888	SYN	2	If a link-up SYN interface was disabled and then enabled again, or if the PPP link over that interface was reset, then the ifOperStatus would change to down and would not come back up again. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00010428	Switch	2	If 0.0.0.0 was specified as an IP address for a VLAN interface, the incorrect VLAN ID was written into the hardware routing table. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y
CR00013548	EPSR	2	Previously, if EPSR failed over, and some of the ports in the EPSR ring were trunked, and there were ARPs present on the non-master port, the ARPs would not be deleted. This meant that connectivity could be lost when the ring switched back. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–
CR00016205	Firewall	2	The firewall did not allow any incoming traffic destined for a non-policy interface, including the local interface. This issue has been resolved. The firewall now allows traffic that comes from a private trusted interface and is destined for a local interface.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00016331	Eth	2	With some link partners, an AR750S Ethernet port would stop receiving packets after some hours or days, and a link state cycle or interface reset was required to restore operation. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00017519	VLAN	2	ARP packets were not processed if they had been tagged with an 802.1p priority value. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017540	Switch, Classifier	2	On AT-8948 and AT-9900 series switches, if a classifier matched on VLAN ID or interface, the switch did not correctly classify traffic. This stopped hardware filters or QoS policies from working if they used such classifiers. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–
CR00017750	IP Gateway	2	When an IP interface went down, and the switch received traffic on another interface that was destined for the down interface's IP address, the switch no longer processed that traffic locally. Instead, it sent the traffic out its default route. For example, if vlan1 had an IP address of 192.168.1.1 and the switch received a ping on vlan2 for 192.168.1.1, then the switch would route the ping out its default route, instead of processing the ping packet and sending a ping reply message back. This issue has been resolved. Traffic that is directed at an IP interface will now be processed regardless of the link state of the interface itself.	–	–	–	–	–	–	–	–	Y	Y	–
CR00017751	IGMP	2	Previously, IGMP packets that had a source IP address of 0.0.0.0 were not accepted. This issue has been resolved. Such packets are now accepted and processed.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017767	Switch	2	When the Ethernet interface of an AR770S router was under very heavy load it could, very occasionally, enter a mode which had a high latency for packets transmitted over the interface. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00018035	Log	2	After changing the destination of the permanent or temporary logs to syslog , the router or switch would sometimes reboot when displaying the dynamic configuration. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018137	Switch, VLAN	2	Previously, multicast limiting did not limit the number of destination look-up failure packets or multicast packets destined to reserved IP multicast addresses. In a correctly-functioning network, rates of these packets are very low, but in a network with a loop, rates can be very high. This issue has been resolved. Multicast limiting now includes such packets.	-	-	-	-	-	-	-	-	-	-	Y
CR00018141	Switch	2	CPU utilisation could become very high under circumstances in which the switch needed to learn a large number of entries. For example, this could occur during a reboot when large numbers of MAC entries require learning. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y
CR00018184	DHCP	2	Previously, the router or switch did not have a minimum length for the Options field of DHCP messages. This conformed to RFC 2131, which states that the length of the Options field is variable, but did not conform to RFC 1531, in which the field has a minimum length of 312 bytes. This issue has been resolved. To maintain interoperability with pre-RFC 2131 DHCP clients, the router or switch now pads the Options field to 312 bytes if it is less than this.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00018270	Switch	2	When aging out FDB MAC entries on x900-48 series switches, it was possible for the FDB entry to be erased while there were still references to it. This could result in L3 switched traffic with a destination MAC of 00-00-00-00-00-00. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	-	-
CR00018700	OSPF	2	When a physical IP interface had multiple logical interfaces running on it and the physical interface's status changed, OSPF only recorded the status change of the first logical interface. For example, if the physical interface was down and came back up, OSPF would only give the first logical interface a status of up; it would leave the other logical interfaces down. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018751	Firewall	2	The firewall sometimes rebooted when using ENAPT, especially if FTP was being run though the firewall. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00018752	Switch	2	An AR770S router could reboot when it was processing a very heavy traffic load in its CPU. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00018941	IP Gateway	2	When deleting an IP RIP interface or disabling an IP interface with RIP running on it, the router or switch would stop responding and reboot after 5 minutes. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00018943	Switch	2	With 1000Base SFPs installed, the AR770S Eth ports failed to establish a link on restarting when receiving a moderate amount of traffic. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00019273	BGP	2	Once a BGP peer had received updates from another peer, it was not possible to use the commands delete bgp net or delete bgp import to remove a locally-imported route from the BGP RIB. This issue has been resolved. These commands will now work at all times.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00019351	TPAD, X25T	2	Multiple concurrent TPAD transactions could cause the router or switch to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00019542	Eth	2	With some link partners, an AR415S Ethernet port would stop receiving packets after some hours or days, and a link state cycle or interface reset was required to restore operation. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00019713	OSPF	2	<p>If two or more ECMP routes from Type-5 LSAs were learned by the router or switch, only the route from the LSA with the highest Router ID would be inserted into the IP route table.</p> <p>This issue has been resolved. All routes will now be inserted.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007089	PRI	3	<p>The following issues occurred with testing PRI interfaces:</p> <ul style="list-style-type: none"> ■ When the commands enable pri=x test=y and disable pri=x test=y were entered, the router or switch did not display an "Operation Successful" message. <p>This issue has been resolved.</p> <ul style="list-style-type: none"> ■ The output displayed by the "?" help for enable pri=x test=? incorrectly said that the maximum value was 11. <p>This issue has been resolved. The "?" help now returns the following message:</p> <pre>required - decimal in the range 1 to 7 (for E1) 1 to 9 (for T1)</pre> <ul style="list-style-type: none"> ■ When show pri=x test was entered, the router or switch displayed an error message instead of the table of test switches. <p>This issue has been resolved.</p> <ul style="list-style-type: none"> ■ When disable pri=x test was entered with no value on the test parameter, the router or switch displayed an error message instead of disabling all current tests. <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007499	VRRP	3	Previously, if a VRRP virtual router was enabled but not connected to anything (for example, no ports in the VRRP VLAN were connected), and the VR was disabled by using the command disable vrrp=n , the error message "Error (3088271): VR n is already disabled" was displayed. This issue has been resolved. This incorrect error message no longer displays.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00007870	IP Gateway	3	The following issues occurred with ICMP Router Advertisement: <ul style="list-style-type: none"> ■ When the feature was enabled, four initial advertisements were sent instead of three, as defined in RFC 1256. ■ The advertisement counter was incremented incorrectly when advertisements were sent on a down interface. This resulted in no advertisements being sent at all. ■ If an advertisement interface was added and then deleted, the interface could not be added again. These issues have been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	Y
CR00007880	LAPB, MIOX, X25-T, Core	3	If the access link to an X.25 network was unstable and suffered outages frequently, it was possible for X.25 calls to become locked up so that data was not successfully transferred. When this happened, the call needed to be manually taken down before normal operation would resume. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00010517	Firewall	3	When the firewall deny event table filled up, the oldest deny event was pushed out by the next new one, even if the old event had not finished. This meant that the old attack was never recorded as having finished, and prevented the firewall from recording that attack again, even after the associated session had closed. This issue has been resolved. The firewall now ends the event as if the event had timed out and finished.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010575	Classifier	3	If the command create classifier=x innervlanid=y was entered, then the configuration from show config dynam or create config displayed the command as create classifier=x innervlanid=y innertpid=8100 , even though the entered command had not specified the innertpid value. This issue has been resolved. The command create classifier=x innervlanid=y no longer sets the innertpid value.	–	–	–	–	–	–	–	–	Y	Y	–
CR00011170	STP, MSTP, Switch	3	Previously, a topology change could result in a mismatch between the switch's software and hardware forwarding database. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00012479	IPv6, TCP	3	Issues in the IPv6 implementation of TCP meant that routers or switches running SSH for IPv6 could reboot under unusual circumstances. These issues have been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00013213	Triggers	3	The command create trigger time accepted invalid dates such as 00-dec-2000. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013772	MSTP	3	If a switch was configured for MSTP with the protocol version set to RSTP, and the switch was connected to a switch that was configured for MSTP with the protocol version set to MSTP, then a loop could occur. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
CR00013775	Firewall	3	When a host on a private firewall interface attempted to ping an unreachable host on a public firewall interface and received "destination unreachable" reply messages created by the firewall, the firewall would create firewall sessions for the packet flow that would time out after 600 seconds. This issue has been resolved. The firewall no longer creates sessions for locally generated "destination unreachable" reply messages.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014278	Firewall	3	When a private LAN interface was brought down then up again, the firewall did not apply NAT to locally generated packets, such as pings. This meant ping replies could not be returned. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00015160	Core	3	It was not possible to enable link trapping on dynamic interfaces. The command to do so (enable interface=dynamic linktrap) returned an error. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015870	Firewall	3	It was possible to enter the same firewall rule multiple times. The duplicate entries would cause the firewall to renumber the rules, leaving multiple copies of the same rule in the configuration. This issue has been resolved. It is no longer possible to enter a rule that is identical to an existing rule.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00015986	VRRP	3	The router or switch could reboot if it was configured with a very large number of VR instances, and each of these VR instances was configured to monitor an interface. In other words, this occurred when adding a large number of VRs by using commands like the following example: create vrrp=106 over=vlan1 ipaddress=192.168.1.109 priority=200 add vrrp=106 monitoredinterface=eth0 This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016768	IPsec, Software QoS	3	If a Software QoS DAR was configured in a traffic class that was attached to an IPSec tunnel interface, the dynamic classifiers were not created or assigned to the traffic class correctly. This issue has been resolved.	Y	Y	Y	Y	–	–	–	–	–	–	–
CR00017240	Switch	3	If there were a large number of IGMP snooping groups and the switch received an IGMP query or other All Router traffic, then it could experience an STP topology change. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017548	Switch, VLAN	3	<p>Previously, when using subnet-based VLANs, only IP traffic matching the source IP network was classified into the subnet-based VLAN. This did not include ARPs.</p> <p>This meant that subnet-based VLANs only worked if all traffic flow was between ports in the same subnet-based VLAN, or if static ARP entries were configured.</p> <p>This issue has been resolved. You can now use a hardware filter to send ARP packets to the CPU, which will process them appropriately. This means that if you use subnet-based VLANs, you also need to add the following hardware filter:</p> <pre>create classifier=1 ethformat=ethii-untagged protocol=0806 add switch hwfilter=1 classifier=1 action=discard,copy</pre>	-	-	-	-	-	-	-	-	Y	Y	-
CR00017692	Core	3	<p>Stack dump information was not available in the show debug or show system dump commands after a fatal exception.</p> <p>This issue has been resolved.</p>	-	-	Y	-	-	-	-	-	-	-	-
CR00017744	Switch	3	<p>When switch ports were under a heavy traffic load, BPDUs could become corrupted (the CRC was missing from the end of the packet).</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	Y	-	-
CR00017851	Firewall	3	<p>When using policy routing in conjunction with Firewall NAT, a policy-routed packet could be sent over an interface while the IP NAT rule that was applied would belong to a different interface. This would result in the packet having a mis-matched source IP address for the interface it was forwarded over.</p> <p>This issue has been resolved. When using policy routing and Firewall NAT, the source address on the resulting forwarded packet will now follow the IP NAT rule attached to the interface over which the packet is forwarded.</p>	Y	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018017	DHCP	3	<p>When a DHCP client was communicating with a DHCP server through a BootP relay, when the client attempted to re-new its address allocation by using unicast DHCP renew messages, the DHCP server would drop the messages and not reply. This forced the client to resort to using a broadcast DHCP discover message.</p> <p>This issue has been resolved. The DHCP server will no longer drop the unicast DHCP renew messages.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00018018	Firewall	3	<p>The SIP ALG was causing a problem when a SIP server on the private side of the firewall was redirecting an incoming call from an endpoint on the public side back out to another endpoint on the public side.</p> <p>The problem was that as the SIP ALG processed the outgoing SIP Invite (sent by the private-side SIP server to the eventual call recipient) it replaced the IP address of the originating endpoint by the public IP address of the firewall. Therefore, when the call connected, the receiving endpoint sent its voice data to the public IP of the firewall, instead of to the originating endpoint. Hence the originating caller heard no sound from the answering caller.</p> <p>This issue has been resolved, so that the SIP ALG now checks whether the IP address of the originating endpoint is on the public side of the firewall, even if the Invite packet came from the private side. If the originating IP address is on the public side of the firewall, the SIP ALG does not change it.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00018034	Switch	3	<p>On 48-port switches, hardware filters that used a classifier with the eport parameter did not always filter traffic correctly.</p> <p>This issue has been resolved.</p>	–	–	–	Y	Y	Y	Y	Y	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018182	PKI	3	<p>Previously, the PKI certificate timestamp was only verified at router or switch initialisation. This caused problems when the time changed, for example because of NTP or if the router or switch had no battery backup (so the time defaulted to 01-Jan-1999 after a reboot). In either situation, the timestamp updates were not communicated to the PKI certificate code so the certificates remained valid or invalid depending upon the initial timestamp check.</p> <p>This issue has been resolved. PKI periodically verifies the certificate timestamps and automatically validates or invalidates the certificate.</p> <p>Also, the show pki command output has been updated to include all the debug options (some were missing) and to improve the output.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00018431	Core	3	<p>SNMP access to the MIB object ifInOctets on the Eth port of an AR770S router did not get the actual updated value unless the value was first refreshed with the show interface=eth counter command.</p> <p>This issue has been resolved.</p>	–	–	Y	–	–	–	–	–	–	–	–
CR00019012	Firewall	3	<p>On very rare occasions, the router or switch could reboot when running as a firewall and using passive FTP.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00019020	GUI	3	<p>In some circumstances, the VPN wizard did not recognise some bundle licences. This issue affected firewall licence recognition.</p> <p>This issue has been resolved.</p>	Y	–	–	–	–	–	–	–	–	–	–
CR00019575	Firewall	3	<p>On rare occasions, the firewall rebooted when processing RTSP or FTP TCP streams.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00019703	L2TP	3	<p>When the router or switch was acting as an LNS, it was possible for it to get into a state where it has an active and an inactive L2TP tunnel both tied to one PPP connection. Previously, when the inactive tunnel timed out, the router or switch closed the PPP connection. This situation with two L2TP tunnels arose when the LAC removed the tunnel in a way that made it unable to notify the LNS (for example, if there was a brief network outage between the LNS and the LAC). Therefore the LNS kept the tunnel up. When the LAC reactivated the call, it created a second tunnel tied to the same PPP connection. This was because L2TP calls could be attached to PPP connections which were already associated with an L2TP call and were active.</p> <p>This issue has been resolved. L2TP calls can no longer be attached to active PPP connections that are already associated with an L2TP call.</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Level 4

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00012634	QoS, Switch	4	<p>QoS sometimes marked traffic red when no metering parameters had been specified and therefore all traffic should have been green. However, the switch did not drop the red-marked traffic, because metering had not been configured.</p> <p>This issue has been resolved.</p>	–	–	–	–	–	–	–	–	Y	Y	–
CR00013088	IPv6	4	<p>When an ICMPv6 time exceeded packet was sent out, the InTimeExcds counter was incremented, when the OutTimeExcds should have been incremented.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013774	Switch, MSTP	4	If MSTP was enabled and a port was set as the mirror port, it was possible for the switch to send BPDUs out of this port. Note these BPDUs were originated by the switch, not mirrored from another port. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
CR00013916	Switch	4	For the ingresslimit and egresslimit parameters of the set switch port command, the output of the “?” help previously said that the range of values was 0 to 4294967295. This issue has been resolved. The “?” help output now gives the correct ranges, which are: ■ 1000 to 127000 (in kbps) for 10/100 Mbps ports ■ 8 to 1016 (in Mbps) for 1 Gbps ports	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00015655	User, RADIUS	4	Previously, the router or switch did not log a message if RADIUS authenticated a user logging in over telnet but RSO rejected the login. This issue has been resolved. A message is now logged, with module USER, type RSO, and subtype RJCT. The message reads “Remote Security Officer access rejected from user <name> at <ip-address>.”	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017449	Switch	4	The set switch port speed command incorrectly accepted a value of 1000mhalf for tri-speed copper SFP ports. This issue has been resolved. If you enter 1000mhalf , the switch displays an error.	–	–	–	–	–	–	–	–	–	Y	–
CR00017971	Utility	4	The “?” help for some parameter options (including add igmp filter=id group=address action=?) did not show all the available options. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010614	IP Gateway	-	Support for ICMP Router Discovery, as described in RFC 1256, has been added to routers, and to AT-8948, x900-48, and AT-9900 series switches. For more information, see “ICMP Router Discovery Advertisements (CR00010614)” on page 163 Note that the other layer 3 switches already supported this feature.	Y	Y	Y	–	–	–	–	–	Y	Y	–
CR00015525	ADSL, Core	-	With this software version, AR440S routers with a hardware revision of M1-2 (or later) will support ADSL2 and ADSL2+ connections. You can see the hardware revision of a router by entering the command show system and checking the “Rev” column for the “Base” board. When running this software version, AR440S routers with rev M1-2: <ul style="list-style-type: none">have the following new options for the command set adsl standard: adsl2 connect only to devices offering ADSL2 adsl2plus connect only to devices offering ADSL2+ auto2plus connect at ADSL2+ if this is offered by the other end device (CO), or otherwise automatically fall back to what is offeredhave a default ADSL standard setting of auto2plusbehave as they currently do for other ADSL standard settings When running this software version, existing AR440S routers with a hardware revision of M1-1 or earlier: <ul style="list-style-type: none">do not have the new options adsl2, adsl2plus, or auto2plus for the command set adsl standardstill use the existing default ADSL standard setting of auto, which allows automatic fallback connection for ADSL standards only.	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016978	STP, MSTP, Switch	-	STP and MSTP debugging has been enhanced to: <ul style="list-style-type: none"> ■ make it easier to see state information, and ■ only display information about Topology Change messages. For command syntax and output details, see “STP and MSTP debugging enhancements (CR00016978)” on page 167.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00017018	Classifier, DHCP snooping	-	This enhancement enables you to act on traffic that is received on an uplink port and is destined for a particular DHCP client. You can use the new functionality, for example, to track how much traffic each user receives via an uplink port. This enables you to track traffic usage at the uplink port, even if destination IP addresses are dynamically assigned by DHCP and traffic for multiple users is in the same VLAN. <p>For command syntax and more information, see “Acting on traffic destined for a particular DHCP client (CR00017018)” on page 170.</p>	-	-	-	-	-	-	-	-	Y	Y	-
CR00018144	IPv6	-	Routing Header type 0 has been deprecated for IPv6 due to security concerns, as described in the Internet Draft at www.ietf.org/internet-drafts/draft-ietf-ipv6-deprecate-rh0-01.txt . <p>When the router or switch receives a packet addressed to it that contains RH type 0, it now responds as if it does not understand the header, as specified in RFC 2460. That is, it ignores the header if the number of segments left is zero, or it replies to the sender with an ICMPv6 incorrect parameters error message.</p>	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018346	VLAN	-	<p>This enhancement adds a new parameter nestedoverride to the command add vlan port.</p> <p>The nestedoverride parameter allows you to add the port to a non-nested VLAN as a tagged port even if the port has already been configured as a customer port in a nested VLAN. The vlan parameter specifies the non-nested VLAN to which you want to add the port. You must also specify frame=tagged. The port will behave as a normal customer port for the nested VLAN, and an egress-only port for the non-nested VLAN:</p> <ul style="list-style-type: none"> ■ Frames received on the port and tagged for the nested VLAN will be sent to the core ports of the nested VLAN, as normal. ■ Frames received on the port and tagged for the non-nested VLAN will be sent to the core ports of the nested VLAN, and will not be sent to other ports of the non-nested VLAN. ■ IGMP frames received on the port and tagged for the non-nested VLAN will be processed according to the IP multicasting configuration, instead of being discarded. ■ Frames received on other ports of the non-nested VLAN will be transmitted from the port as tagged frames of the non-nested VLAN according to the FDB/multicast rules. <p>The nestedoverride parameter creates a non-standard configuration, and care should be taken when using this parameter in a live network. The nestedoverride and uplink parameters are mutually exclusive and cannot be specified in the same command.</p> <p>An example configuration would be:</p> <pre> create vlan=v22 vid=22 nested create vlan=v20 vid=20 add vlan=v22 port=1 nested=customer add vlan=v20 port=1 frame=tagged nestedoverride </pre>	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018438 CR00019826 CR00019827	BRI	-	This software version supports the new AR021v3 BRI PIC. The user interface for this PIC is the same as for the AR021v2, except that output of the command show bri counters is simpler—there are no IOM counters and fewer D channel counters.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00019152	Bridging	-	The number of ports supported by Bridging has been increased from 32 to 512.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00019377	L2TP	-	Previously, the length of the L2TP call name was limited to 15 characters. This limit has been increased to 19 characters.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00019749	OSPF	-	This enhancement increased the maximum acceptable payload size of an OSPF Link State Update from 1452 bytes to 1992 bytes. As an example, previously the maximum number of Router LSAs that could be received in one Link State Update was 119. This has increased to 164.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Features in 291-10

Software Maintenance Version 291-10 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-10 for that product series.
- “-” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016759	Switching, DHCP Snooping	2	<p>Enabling DHCP snooping (correctly) adds a hardware filter to all untrusted ports, to block all IP traffic coming from those ports. Previously, disabling DHCP snooping did not delete these filters. This meant that the switch dropped all IP traffic from the previously-untrusted ports until the switch was restarted.</p> <p>Also, attempting to manually delete the hardware filters did not actually remove them.</p> <p>These issues have been resolved. The switch now removes the filters if you disable DHCP snooping or manually delete the filters.</p>	-	-	-	-	-	-	-	-	Y	Y	-
CR00018655 CR00018656	IP Gateway	2	<p>If the user did not specify the destination and dmask parameters when entering the set ip filter command, the destination and dmask of the filters were reset to any.</p> <p>Also, it was not possible to delete an IP filter by using the delete ip filter command, even when all required parameters were present.</p> <p>These issues have been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018663	Switching	2	The resolution to CR 444 meant that packets processed by the CPU are now subjected to the same filtering as packets switched in hardware. However, this filtering did not always return the expected results. Sometimes its IP address matching was incorrect, and it did not correctly process filters with an action of nodrop . These issues have been resolved.	-	-	-	Y	Y	Y	Y	Y	-	-	-
CR00018691	OSPF	2	On a router or switch with OSPF redistribution enabled, OSPF did not redistribute the interface route when an interface came up (for example, after a reboot). This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00018693	QoS	2	QoS policies, traffic classes, and flow groups could not have an ID number of 0 (zero). This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00018778	IP NAT, Firewall	2	When using IP NAT, the router or switch would reboot when processing TCP SYN packets. This issue only occurred with IP NAT, which is configured by using the add ip nat command. It did not occur with firewall NAT. This issue has been resolved.	Y	Y	Y	-	-	-	-	-	-	-	-

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018514	Ping	3	Traceroute (the trace command) did not work. It returned the error “The destination is either unspecified or invalid” even if the destination was reachable. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

No level 4 issues

Enhancements

No enhancements

Features in 291-09

Software Maintenance Version 291-09 includes the enhancement in the following table, which is available for x900-48FE and x900-48FE-N switches.

Level 1-4

No level 1-4 issues

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00018530	Core	-	<p>CPU fan monitoring is now disabled by default on x900-48FE and x900-48FE-N switches. Monitoring the fan is unnecessary unless an accelerator card is installed on the switch, so disabling monitoring reduces the number of messages that the switch displays and logs.</p> <p>To enable monitoring, use the command:</p> <pre>enable cpufanmonitoring</pre> <p>To disable it again, use the command:</p> <pre>disable cpufanmonitoring</pre> <p>When monitoring is enabled, the command show system displays the CPU fan status in the entry labelled "Main fan".</p> <p>Note that this behaviour is already available on AT-8948 switches.</p>	-	-	-	-	-	-	-	-	Y	-	-

Features in 291-08

Software Maintenance Version 291-08 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-08 for that product series.
- “-” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00000444	Switching, IGMP, IP Gateway	2	If a packet should have matched a hardware filter with a deny action and have been discarded, but an IP routing entry had not yet been learnt for the packet, then the packet was not discarded. This issue has been resolved and the packet is now discarded.	-	-	-	Y	Y	Y	Y	Y	-	-	-
CR00000484	Switching	2	When a nodrop action was specified on a port as part of an L3 filter, it was observed that the port was still dropping packets. This was observed after the ARP entry for the destination IP expired from the switch's L3 table. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	-	-	-
CR00001231	Firewall	2	The router or switch sometimes recorded more events in its deny event queue than was specified by the detail parameter of the set firewall policy attack command. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00003495	Classifier	2	<p>The following issues existed with classifiers:</p> <ul style="list-style-type: none"> ■ classifiers matching protocol=ipv6 and ipprotocol=icmp could be created more than once ■ classifiers matching protocol=ipv6 and ipprotocol=1 could be created but were meaningless because 1 represents IPv4 ICMP ■ classifiers matching protocol=ip and ipprotocol=58 could be created but were meaningless because 58 represents IPv6 ICMP. <p>These issues have been resolved.</p> <p>Also, classifiers now default to protocol=ip (IPv4) if:</p> <ul style="list-style-type: none"> ■ no value is specified for the protocol parameter, or ■ protocol=any and ipprotocol=icmp. 	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00004018	VLAN	2	<p>Removing then re-adding ports to a Nested VLAN, with rapid STP enabled, caused the port in the Alternate Discarding state to leak a small number of packets.</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	-	Y	-
CR00005472	BGP	2	<p>When BGP was in the OpenSent state and it received an out-of-sequence message (such as a KeepAlive message), BGP would return to the Idle state.</p> <p>This issue has been resolved. BGP now sends a notification message to the other BGP peer, as expected.</p>	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00005812	IP Gateway	2	<p>When the router or switch received an IP packet whose length was greater than the MTU on the outgoing link, and the packet contained an IP option that was not designed to be fragmented (such as Timestamp), then the resulting constituent fragments would have incorrect IP header lengths.</p> <p>This could lead to data corruption.</p> <p>On routers, this issue applied to all routed packets. On switches, it applied to packets processed by the CPU, not to packets switched in hardware.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007178	RIPng	2	<p>The following issues occurred with RIPng:</p> <ul style="list-style-type: none"> ■ RIPng dropped requests from peers with non link-local addresses. ■ for a solicited response, if the routes did not exist on the device, RIPng returned a metric of 0 for them instead of returning a metric of 16 ■ RIPng performed split-horizon checking for solicited responses ■ RIPng used the link-local address to respond to all requests, even if the request used a non link-local address and therefore the reply should have also used a non link-local address <p>These issues have been resolved.</p>	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00008847	Install, MIB	2	<p>Previously, the MIB objects configFile and createConfigFile would return the current configuration file, and the MIB object currentConfigFile would return 'no such object'.</p> <p>This issue has been resolved. The objects configFile and createConfigFile now return the boot configuration file. The object currentConfigFile now returns the current configuration file.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00009473	Classifier	2	<p>The output of the show classifier=number command did not show the protocol number.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010654	Firewall	2	<p>When adding a firewall application rule, it was possible to specify FTP as the application but not specify the command parameter. This meant that the rule would allow all FTP commands through, even if action=deny had been specified.</p> <p>This issue has been resolved by making the command parameter mandatory when the application is specified as FTP.</p>	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00010951	PPP	2	<p>If the router or switch received an LCP packet with an unrecognised code, it responded with a CodeReject packet of incorrect length that did not respect the established MRU of the peer.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010967	PPP	2	If the router or switch received an LCP packet with an unrecognised protocol, it responded with a ProtocolReject packet of incorrect length that did not respect the established MRU of the peer. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010968	PPP	2	When the established Maximum Receive Unit (MRU) of the remote PPP peer was greater than the established MRU of the local PPP peer, Echo Reply packets did not respect the established MRU of the remote peer. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011231	Core	2	In most circumstances the stack dump for an AR7x5 router was invalid and did not contain complete information about the cause of a reboot. This issue has been resolved.	-	Y	-	-	-	-	-	-	-	-	-
CR00012218	VPN, GUI	2	Enabling VPN (IPsec) on the GUI caused the GUI VPN page to stop displaying information about some or all of the existing VPN policies. This issue has been resolved.	Y	-	Y	-	-	-	-	-	-	-	-
CR00012727	OSPF	2	Sometimes when a type 7 external LSA was translated to a type 5 external LSA the forwarding address was set to 0.0.0.0 in the translated type 5 LSA. This issue has been resolved, so that the forwarding address is always copied from the type 7 LSA being translated.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012751	OSPF	2	When the router or switch is acting as an area border router and one of the areas is an NSSA (Not So Stubby Area), the router or switch will create a default route for the NSSA and inject this into the NSSA. Previously, the router or switch was also redistributing this route into other areas as a static route when static route redistribution was turned on. This was not desirable behaviour. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00012871	TTY	2	Unexpected characters could appear on the terminal emulator display when the column size was set greater than 80 and the user edited a command that spanned more than one line of the display. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013597	DVMRP, Frame Relay	2	If a frame relay interface was configured as a DVMRP interface, then the DLC value was not correctly generated in output of the command show config dynam or in the configuration script generated by the command create config . This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-	-
CR00013660	Core, SNMP	2	Previously, SNMP returned an incorrect product ID number for AR750S-DP routers. This issue has been resolved. The value of the sysObjectID object is now 80 for AR750S-DP routers.	-	-	Y	-	-	-	-	-	-	-	-
CR00013735	LACP, Switching	2	When moving ports from an LACP-controlled trunk to a manually-configured trunk, ports were incorrectly set in an STP blocking state. Therefore, traffic would not flow over the trunk. This issue has been resolved. Note: When you move ports from an LACP-controlled trunk to a manually-configured trunk, you must delete the ports from LACP.	-	-	-	-	-	-	-	-	Y	Y	-
CR00013763	OSPF	2	If the obsolete command set ospf rip=both was entered, the router or switch correctly automatically replaced it with the following two commands in the dynamic configuration: add ospf redistribute protocol=rip set ospf rip=export However, if the command create config was used to save the configuration, after system start-up the configuration file did not contain the command add ospf redistribute protocol=rip . This meant that OSPF stopped redistributing RIP routes after a reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013778	IPv6	2	If a user shortened the prefix length of an IPv6 interface address, then lengthened it, it became impossible to change the prefix length again. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00013893	MSTP	2	Executing the commands disable mstp port=number or enable mstp port=number would not disable or enable the port on all MSTIs. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00013982	L2TP	2	An L2TP call could be deleted when still attached to the PPP interface. Doing this caused the router or switch to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-	-
CR00014044	IGMP	2	When large numbers of multicast streams were passing through the switch and there was no multicast routing protocol running (such as PIM or DVMRP), the CPU would experience regular periods of extended high utilisation. This could result in lost control packets and network instability. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y
CR00014146	TTY	2	When a file was redirected (for example, by a trigger), if the mail hostname was not available or not configured, the router or switch would reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014230	TTY	2	If the built-in editor was used to delete the last line of a file, the router or switch could reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014295	IGMP	2	IGMP snooping would process IGMP protocol packets that had incorrect IP TTL fields (i.e. that had values other than 1). This issue has been resolved.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014320	OSPF	2	Occasionally, when OSPF was started, not all the Type-7 LSAs were translated into Type-5 LSAs. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014827	PIM6	2	If an IPv6 accelerator was used, and the upstream router forwarded IPv6 multicast data just before the prune limit timer expired, then the downstream router sometimes did not send the prune until significantly after the timer expired. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00015169	MSTP, GUI	2	Using the web-based GUI to set the Point-to-Point Link in the MSTP CIST Port configuration to a non-default value would generate an error. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00015805	ISAKMP, IPv6	2	During the boot up, the router or switch waited 5 seconds before beginning ISAKMP prenegotiation. For VPN tunnels over IPsec for IPv6, this was not long enough for the router or switch's interfaces to come up before prenegotiation began. Also, the router or switch did not obtain the most recent active ISAKMP SA when multiple SAs existed. These issues have been resolved. The router or switch now waits 6 seconds, and obtains the most recent SA and uses that for Phase 2 negotiations.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00015964	Switching	2	If the switch had a large number of routes in its forwarding database (FDB), and the command show switch fdb was used to display the contents of the FDB, and the switch's CPU was busy at the time, then the switch sometimes rebooted. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00016262	Load	2	When attempting to upload files from the switch using TFTP to an IPv4 server address, the router or switch reported an error if IPv6 was not enabled. It was not possible to upload files using TFTP to an IPv6 server address at all. These issues have been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016340	DHCP Snooping	2	DHCP Snooping has been enhanced to operate in a customised VLAN ID translation (VID translation) environment. Previously, DHCP Snooping was not supported with VID translation. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00016587	IPv6	2	The timer that governs the interval between repeated neighbour solicitation messages could only be configured by using the ndretrans parameter of the set ipv6 nd command, and not through router advertisements that the router or switch received from other routers. This issue has been resolved. Instead of using the ndretrans parameter of the command set ipv6 nd , use the retrans parameter to configure the timer interval. Also, routers or switches acting as hosts will now correctly update their timer values to the value specified in any router advertisements that they receive.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016592	DHCP6	2	Previously, it was possible to enter the incomplete commands delete dhcp6 policy=name or set dhcp6 policy=name without specifying any other parameters. This issue has been resolved. If this is done, the router or switch now displays the warning: Warning (2117007): One or more parameters may be missing.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016840	STP	2	Previously, when the switch was a Spanning Tree root bridge in a network and a user raised the switch's root bridge priority enough to stop the switch from being the root bridge, unnecessary delays in convergence occurred. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00016956	IP Gateway	2	The set ip filter command would not accept the protocol parameter. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016964	ISAKMP	2	When the router or switch negotiated an IPsec tunnel with RFC3947 NAT-T, its NAT-OA payload had two bytes of reserved fields after the ID field instead of the three bytes specified by RFC 3947. This could prevent the tunnel from working properly when the tunnel was between an Allied Telesis router or switch and some other vendor. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00016985	ATM	2	If a PPP instance was destroyed after an attached ATM channel had been modified using the set atm channel command, the router rebooted. The router could also reboot if an ATM channel was deleted under similar circumstances. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-
CR00016989	IPsec	2	AlliedWare IPsec would not interoperate with Microsoft Windows Vista VPN clients. This was because Microsoft changed the IPsec behaviour in Vista such that Vista's private local IP address is sent as the local identification instead of an FQDN. When an IPsec tunnel between AlliedWare and Vista was brought up, the hosts could not communicate. This issue has been resolved. AlliedWare IPsec can now communicate with peers that send their private local IP address as the local identification.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00017081	Classifier	2	The show classifier command did not allow users to display only the classifiers that had their IP source address and MAC source address parameters set to dhcpsnooping . This issue has been resolved. For example, the command show classifier ipsa=dhcpsnooping now displays those classifiers that have their IP source address set to dhcpsnooping . Also, it is no longer possible to create two identical classifiers with DHCP snooping parameters.	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017093	Firewall	2	When the router was acting as a firewall and performing DNS relay, it used the local IP interface private address as the source address for some packets that it sent out the public interface. When the router acts as a DNS relay, it receives DNS requests from the private interface and sends a new packet on the public interface. These new packets were given the wrong address. This issue has been resolved. Such packets now have their source address set to the public interface address as required.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00017226	IPsec	2	If an IPsec tunnel with no encryption (NULL) was negotiated in AlliedWare over NAT-T, the ESP packets did not contain an RFC 3948 compliant checksum. This means that some vendors may have discarded packets sent by the AlliedWare peer over such a tunnel. This issue has been resolved. Note the null encryption is useful for debugging the traffic over an IPsec tunnel and should not be used in a working IPsec solution.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00017227	IPsec	2	An IPSec checksum recalculation error occurred with UDP traffic when the ESP encapsulation was added. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00017255	Switching	2	Previously, trunk members were given the STP state in hardware of port 1, instead of having the STP state of the lead port in the trunk. The software state (as displayed with the command show stp port) was correct. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	-	-	-
CR00017256	Switching	2	When using multi-homed IP interfaces on a VLAN, it was possible that L3 hardware switching would stop for all multi-homed interfaces on that VLAN, if one of the multi-homed interfaces was removed or went into an administratively down state. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017337	Switching	2	It was possible to set up a classifier that matched MPLS frames at layer 2, but the switch would not correctly match these MPLS frames against the classifier. This issue has been resolved. The switch now correctly matches MPLS frames against such a classifier.	-	-	-	-	-	-	-	-	Y	Y	-
CR00017368	QoS, DHCP Snooping	2	Some small memory access violations existed in DHCP snooping. These violations have been resolved. Also, a new console error message is displayed if a user tries to add a duplicate classifier to a QoS policy. For example, if traffic class 101 belongs to policy 2 and a user tries to add a flow group to traffic class 101 when the flow group's classifier is number 54 and already belongs to policy 2, the following message is displayed: Error (3099297): Duplicate classifier (54) on policy 2. A similar new log message has also been added, which says: Duplicate classifier (<number>) found on <string> <number> Note that a classifier can exist in two separate policies but cannot exist twice in the same policy.	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00017456	IP Gateway	2	The router or switch could reboot when the local interface address had been specified by using the set ip local command, and then the underlying interface from which the local interface took its address was either deleted or had its address changed. In both these cases, the local interface was correctly reset back to an undefined address, but a route to this address was not deleted. This could cause routing difficulties and a reboot when packets for that address were received. This issue has been resolved. The route is now correctly deleted.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017488	Firewall	2	When a VoIP call using SIP was initiated from the public side of the firewall, occasionally the firewall created two UDP sessions for the call with different UDP source ports. This happened if the first packets of the STP (voice data) stream arrived earlier than the 200 OK message that was supposed to establish the session. The result was that the public side caller could not hear the call. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00017518	ISAKMP	2	The router or switch sometimes could not establish a VPN when the remote peer was behind a NAT gateway and the router or switch's remote ID was set to default . This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR00017634	PPP	2	If a PPPoE AC service had been added, but AC mode had not been enabled by using the enable ppp ac command, PADI frames were processed anyway, potentially leading to a reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00017659	TTY	2	Previously, it was not possible to configure a TTY service on the router (by using commands like create service). This issue has been resolved.	Y	-	Y	-	-	-	-	-	-	-	-
CR00017662	Core	2	Stopping and restarting two fans on the switch in a particular order could put the fan fault detection mechanism into a state in which the system LED would not flash for a fan fault. This issue has been resolved.	-	-	-	-	Y	-	-	-	-	-	-
CR00017724	IGMP	2	When the switch had a hardware filter configured that would match and discard a received IGMP packet, IGMP snooping still processed the packet and added the details to its snooping database. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017731	IP Gateway, DHCP	2	<p>When the DHCP server was enabled on a router or switch that also had a local IP interface defined by using the set ip local command, outgoing DHCP server packets would use the set ip local command's IP address as their source address. Furthermore, if the broadcast flag was set to TRUE in the DHCP Discover message that the server was replying to, then the server would send the DHCP Offer packet out the wrong IP interface with the wrong source IP address. Microsoft Windows Vista has the broadcast flag set to TRUE.</p> <p>These issues have been resolved. The DHCP server configuration now ignores any local IP interfaces set by using the set ip local command, and the server now sends the Offer message out the interface that it received the Discover on.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017749	Switching	2	<p>If a multicast route had an odd number of downstream interfaces attached to it, and the last downstream interface was deleted, the second to last downstream interface could experience a loss of packets.</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	Y	Y	-
CR00017816	PIM	2	<p>PIM would sometimes start forwarding duplicate packets from the RP to downstream interfaces if the SPT Bit had been set and had become unset.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
CR00017906	VLAN, MSTP	2	<p>If ports were removed from a VLAN and MSTP was enabled, then the port removal was not included in the configuration displayed by the command show config dynam or saved by the command create config.</p> <p>This issue has been resolved.</p>	-	-	-	Y	Y	Y	Y	Y	Y	Y	-

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00000503	PKI	3	Some PKI commands (including add pki ldap , create pki enroll , and create pki keyupdate) only worked if their parameters were entered in a particular order. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00001106		3	The command add fire policy=name rule=number act=allow int=int ip=ipadd list=filename would incorrectly be rejected, with an error message stating that list and ip were mutually exclusive. This issue has been resolved, so that list and ip can be used together in the same firewall rule.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00001438	TACACS+	3	If TACACS+ was used for authentication and the TACACS+ server went down during an authentication attempt, the router or switch added the attempted login names to the TACACS+ user list (as displayed in output of the show tacplus user command). However, the router or switch correctly did not log users in with those names. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00002587	IP Gateway	3	Sometimes an incorrect error message was printed if a user tried to enable IP multicast switching on a device that did not support it. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	-	-	-
CR00003354	Firewall	3	The firewall message "Port scan from <source> is underway" was repeated more times than messages about other attack events. This could cause confusion. This issue has been resolved. The message is now displayed with the same frequency as other firewall attack event messages.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00003356	Firewall	3	The firewall sometimes did not report that an attack had finished until several minutes after it actually finished. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00004004	File	3	The show file command did not check whether the specified file system was valid. If an invalid file system type was entered (such as show file=abc:*. *), the router or switch reported that no files found instead of reporting that the file system abc did not exist. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00005048	GUI	3	The following issues occurred with the GUI: <ul style="list-style-type: none"> the menu item and related page title for configuring PPPoE and PPPoA interfaces was incorrectly named “PPP”. This issue has been resolved by changing the names to “PPPoE / PPPoA”. the UPnP selection option on the firewall pages did not work. This issue has been resolved. Note that if you want to use the GUI to configure a PPP interface over ISDN, use the Dial-up menu option to do so.	Y	-	Y	-	-	-	-	-	-	-	-
CR00005187	LACP	3	If a user attempted to enable LACP on AT-9800 series switches—which do not support LACP—the switch incorrectly said that the module had been enabled. This issue has been resolved. The switch now displays an error message instead.	-	-	-	-	-	-	-	-	-	-	Y
CR00005894	Classifier	3	Previously, a classifier with protocol=ip matched both IPv4 and IPv6 packets when used with software QoS, instead of only matching IPv4 packets. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-	-
CR00005940	BGP	3	There were several cases in BGP where an error was discovered in an incoming packet, but the incorrect error subcode was reported in the accompanying NOTIFICATION message. Also, NOTIFICATION messages did not contain the aberrant data in their data fields, as required by the RFC. These issues have been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00006303	SNMP	3	On AR725 and AR745 routers, which have no VLAN support, an SNMP Get request for dot1qMaxVlanId or dot1qMaxSupportedVlans incorrectly returned a value. This issue has been resolved.	-	Y	-	-	-	-	-	-	-	-	-
CR00006613	Bridge	3	Predefined bridge protocols XEROX PUP and PUP Addr Trans with the encapsulation of EthII and protocol type 0x0200 and 0x0201 are invalid and obsolete, since they are less than the minimum ETHII protocol type of 1500 (decimal). Bridging with these protocols could cause the router to reboot. This issue has been resolved by replacing the predefined protocol types with the more modern equivalents 0x0a00 and 0x0a01. Also, if you enter a protocol type less than the minimum, the router now displays an error message.	Y	Y	Y	-	-	-	-	-	-	-	-
CR00007394	GUI	3	When a user used the GUI to attempt to delete a local interface that was in use by another protocol, the operation (correctly) failed, but the GUI did not display an error message to explain the failure. This issue has been resolved.	Y	Y	Y	Y	-	Y	Y	Y	-	Y	Y
CR00007404	MSTP	3	If a network running MSTP was connected to a network running RSTP and MSTP message debugging was enabled on a switch, the debug output could loop for a very long time with invalid data. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	-
CR00007926	Switching, IP Gateway	3	The x900 series switches did not send an ICMP Redirect packet when they received a packet and the route to the packet's destination was back to the packet's sender. The switches routed the packet back to the source but did not send an ICMP Redirect message. This issue has been resolved. The x900 series switches now send an ICMP Redirect message.	-	-	-	-	-	-	-	-	Y	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00008122	TTY	3	When prompted to enter a file name while using the command line file editing utility, no more than 23 characters could be typed, even if the existing characters were deleted using the backspace key. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00008378	Firewall	3	The command enable firewall notify=port port=asyn-number was not available on switches, only on routers. If a user created a configuration on a router and used this option, the configuration had to be modified if transferred to a switch. This issue has been resolved. The notify=port option and the port parameter are now available on switches. However, these port parameters have been deprecated in favour of the asyn parameters, so warning messages are printed to indicate this if the commands are used.	-	-	-	Y	Y	Y	-	-	-	-	Y
CR00009086	Switching	3	When the commands enable switch port=number automdi and disable switch port=number automdi were executed from a telnet session, some INFO messages were output to the asyn0 console session instead of the telnet session. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	-
CR00010144	STP, SNMP	3	Previously, newRoot and topologychange traps (located at 1.3.6.1.2.1.17.0) were only generated by the bridging module. This has been extended to the STP module. Please note that this applies only to standard STP, not Rapid STP.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00010229	Install, SNMP	3	Previously, MIB objects instRelMajor, instRelMinor and instRelInterim values were only correct for bootrom (default) builds. This issue has been resolved. Now the correct values are returned for these objects when the current install matches the temporary or preferred install.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010306	Install	3	If a user attempted to enter a filename with an invalid format, the resulting error message did not correctly describe the format that should have been used. Also, the router or switch returned an incorrect error message when a user attempted to delete a non-existent release licence file. These issues have been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010315	BGP	3	Previously, it was possible to enter bad BGP peer IP addresses, such as 0.x.x.x, 127.x.x.x and 255.255.255.255. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010465	Switching	3	The "?" help for the command show switch sock=con inst=value showed a maximum value of 4294967295. This issue has been resolved. Valid instance values are 0 and 1.	-	-	-	Y	Y	Y	Y	-	-	-	-
CR00010538	Firewall	3	When firewall events were recorded in the Notify queue (displayed in output of the command show firewall event=notify), the IP address shown would be the address of the very first packet that belonged to that event flow. For example, if 64 host scan packets were required to trigger a host scan event and the first packet had a target IP of 1.1.1.1 and the 64th had an IP of 1.1.1.64, then the IP address recorded would be 1.1.1.1, even though the event was not actually recorded until the 64th packet arrived. Additionally, the source and destination ports in this display would always show as 0. These issues have been resolved. The IP addresses shown are now those of the particular packet that triggered the event notification, and the source and destination ports match the actual ports used by that packet.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00010976	PPP	3	If the router or switch received an Echo-Request that did not comply with RFC 1661, it processed and replied to the Echo-Request. This issue has been resolved. Non-complying Echo-Requests are now ignored.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010979	PPP	3	PPP incorrectly ACKed a LCP ConfigureRequest containing the Magic-Number option with a value of 0. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00010984	PPP	3	If the router or switch received an incorrectly formatted PAP request packet, it used to process the packet. This issue has been resolved—now it silently discards the packet. Also, if the router or switch received a PAP request packet with a zero length user ID, it used to send the packet to the authentication database. This issue has been resolved—now it NAKs the packet.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00011223	Core	3	On AT-8948 and AT-9924SP switches with an empty PSU bay, an SNMP walk through of the fanAndPsPsuStatusTable would display lines for the non-existent PSU, with the value of “no such instance”. This issue has been resolved. The walk through now only includes installed PSUs.	-	-	-	-	-	-	-	-	Y	Y	-
CR00011259	GUI	3	Some of the features supported in the web-based GUI did not have a complete set of online help pages generated for them. This issue has been resolved.	Y	Y	Y	Y	-	Y	Y	Y	-	Y	Y
CR00011315	IP Gateway	3	When the limit for the number of IP interfaces was reached and a user tried to add another IP interface over a VLAN, the router or switch displayed the following misleading error message: Error (3005273): No more VLAN interfaces may be added. This issue has been resolved. The error message is now: Error (3005273): No more IP interfaces over VLANs may be added.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011438	Ping	3	When the router or switch pinged a host whose hostname consisted only of the digits 0-9 and the letters A-F, it treated the given hostname as a hexadecimal IPX address even if the hostname was in the host list. This issue has been resolved. Now, when the router or switch pings a host using a hostname, it checks the hostname in the host list first. If it does not find the host in the host list, then it treats the hostname as an IPX address.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00011824	Firewall	3	When a firewall UDP session starts up, the session timeout should be 5 minutes for the first 5 packets of the session, then change to the configured UDP session timeout value. Previously, the timeout changed after the 6th UDP packet belonging to that session, instead of after the 5th packet. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00012066	IP Gateway	3	The command show ip cassi command is obsolete but was still available. This issue has been resolved. The command has been removed from the command line. To obtain the same information, use the command show conf dyn=ip .	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012168	Classifier	3	Output of the show classifier command displayed only the hexadecimal protocol value for IP SNAP, instead of also displaying the protocol name. This issue has been resolved. The output now displays: 0000000800 (IP SNAP)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012885	OSPF, GUI	3	If there were virtual OSPF interfaces, then the OSPF Interfaces GUI page showed all interfaces as belonging to the backbone area (0.0.0.0). This issue has been resolved.	Y	Y	Y	Y	-	Y	Y	Y	-	Y	Y
CR00013352	STP	3	The help displayed by the command set stp port=all ? listed some parameters twice. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00013494	IP Gateway	3	Once a default local IP address had been set, it could not be deleted. This was because the default interface does not have an interface number, but to delete a local interface, the user must specify the interface's number. This issue has been resolved, by adding an option called default to the delete ip local command. To delete the default local interface's address, use the command: delete ip local=default Note that this resets the interface, including removing its IP address, but does not remove the interface itself.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013543	DHCP	3	<p>If a user attempted to add a policy option to a DHCP policy by using the set command instead of the add command, then the resulting error message did not clearly indicate the cause of the error.</p> <p>For example, entering the command:</p> <pre>set dhcp policy=test arptimeout=234</pre> <p>resulted in the error message:</p> <pre>Error (3070061): ARPTIMEOUT not found.</pre> <p>This issue has been resolved. The error message now reads:</p> <pre>Error (3070279): Option ARPTIMEOUT was not found in policy test or was not added using the ADD DHCP POLICY command.</pre>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013635	Ping, Traceroute	3	<p>In the set trace command, it was possible to specify a minimum TTL value that was higher than the maximum TTL value.</p> <p>This issue has been resolved. The minttl and maxttl parameter are now checked to ensure that the value of minttl is less than or equal to the value of maxttl.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013637	Ping, Traceroute	3	<p>If the value specified for the minimum time-to-live parameter (minttl) of the traceroute command exceeded the value set for the maximum time-to-live parameter (maxttl), the router or switch would attempt to execute the trace rather than generate an error message.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013832	EPSR, SNMP	3	<p>When a user destroyed an EPSR domain, SNMP Requests returned information about the domain even though it no longer existed.</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	Y	Y	-
CR00013920	Ping, Traceroute	3	<p>If a user attempted to perform a traceroute without specifying the address to trace (either in the trace or set trace commands), the router or switch attempted to trace 0.0.0.0.</p> <p>This issue has been resolved. The router or switch now displays an error message.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014103	VRRP, GUI	3	The VRRP priority could not be modified through the GUI—the priority option was there but did nothing. This issue has been resolved.	Y	Y	Y	Y	-	Y	Y	Y	-	Y	Y
CR00014137	PPP	3	A PPPoE Access Concentrator service that had been added by using the acinterface parameter to specify a VLAN (or by using the deprecated vlan parameter) could be deleted without specifying the acinterface parameter (or the deprecated vlan parameter). This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00014159	RSTP	3	RSTP (correctly) only uses the top 4 of the available 16 bits for the bridge priority. If a user enters a value that is not a multiple of 4096, the switch rounds the value down. Previously, the switch did not inform users when it rounded the value. This issue has been resolved. The switch now displays an info message when it rounds the bridge priority. Note that this only happens for RSTP. STP uses all 16 bits for the bridge priority.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00014203	OSPF	3	When OSPF was disabled and a BGP redistribution definition existed, then the obsolete command set ospf bgplimit=limit did not update the limit in the BGP redistribution definition. This meant that the limit was incorrect when OSPF was enabled again. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00014304	LLDP	3	The help displayed for the LLDP port parameter (in such commands as show lldp port=?) incorrectly indicated that the port parameter is a “string 1 to 255 characters long”. The port parameter is instead an Ethernet switch port number or a range of numbers. This issue has been resolved. The help is now correct.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014330	Ping	3	The maximum value for the delay parameter of the ping command was too long. This issue has been resolved by changing the range for the delay from 0-4294967295 to 0-604800. This new maximum is the number of seconds in one week.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014879	Switching, RSTP, SNMP	3	Previously, an incorrect value was returned for the port number when responding to an SNMP Request for MIB object dot1dSTPRootPort. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00015466	Core, Install, PoE	3	The output of the show cpu command on the AT-8624POE switch showed relatively high CPU usage when the device was idle. This issue has been resolved.	-	-	-	-	-	-	Y	-	-	-	-
CR00016183	File	3	If a user attempted to delete a locked file, such as the currently-installed GUI resource file, the router or switch displayed both an operation error message and an operation successful message. This issue has been resolved by removing the incorrect operation successful message.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016429	OSPF	3	Previously, OSPF logged the same message for two separate errors. These errors were when OSPF rejected a database description message because: <ul style="list-style-type: none"> ■ the neighbour was in a state of “down” or “attempt”, or ■ the MTU received from the neighbour was larger than the receiving system could handle. This issue has been resolved. Separate error log messages are now generated for these two errors.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016452	PPP	3	It is valid to use the command create ppp=number to create a PPP interface without specifying the underlying layer 1 interface. However, executing this command, or including it in a boot script, resulted in an error. This issue has been resolved.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016578	IPv6	3	<p>If IPv6 was disabled and a user entered any of the following commands:</p> <ul style="list-style-type: none"> add ipv6 interface add ipv6 6to4 add ipv6 tunnel create ipv6 interface enable ipv6 advertising <p>then the router or switch correctly displayed a warning message to indicate that IPv6 was disabled and also correctly performed the specified configuration. However, it did not display an "Operation successful" message to indicate that the configuration had changed.</p> <p>This issue has been resolved. The router or switch now displays the "Operation successful" message as well as the warning message.</p>	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016735	ATM	3	<p>Sometimes, the router displayed the following error message:</p> <p>Internal Error: speed mismatch causing transmit internal rate underrun error.</p> <p>This was due to a mismatch in the synchronisation between the internal rate of the ATM controller in the CPU and the speed of the ATM PHY connector. This synchronisation mismatch had a small impact on ATM performance. This issue has been resolved.</p>	Y	-	-	-	-	-	-	-	-	-	-
CR00016925	TTY	3	<p>If a user was accessing the router or switch via telnet, and sent a ^P (break) character followed by the character d or D, then the router or switch displayed an unwanted diagnostic message. This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017019	Port Authentication	3	<p>On termination of an 802.1x session, an accounting message is sent to the Radius server. This enhancement implements the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields in the message.</p> <p>Note that this enhancement only applies to ports in single-supPLICANT mode. These fields in the accounting message for ports in multi-supPLICANT mode still all have a value of 0.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00011228	GUI, Switch	4	The Diagnostics > Layer 2 Forwarding Database page of the GUI displayed extra internal (SYS or CPU) entries. This issue has been resolved. The GUI and the command show switch fdb now display the same information.	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00013409	Switch	4	Previously, if you used the ? or Tab keys to obtain help for the set switch ageingtimer command, the resulting help said that valid entries were from 0 to 4294967295. However, the correct range of values is from 16 to 4080 seconds for AR750S routers and from 10 to 630 seconds for AR770S routers. This issue has been resolved. The “?” help now displays the correct ranges.	–	–	Y	–	–	–	–	–	–	–	–
CR00014205	OSPF	4	The command purge ospf did not delete OSPF redistribution definitions. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014302	TTY	4	If the router or switch configuration file contained the command set tty idle , the router or switch produced a corrupted log message when it started up. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00012822	BGP	-	The BGP counter output display has been significantly improved. Also, the command show bgp counter=all now prints out the RIB, UPDATE, DB and PROCESS counters.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016099	MACFF, DHCP Snooping	-	<p>MAC-forced forwarding has been enhanced for use in a hospitality situation, such as a hotel. The enhanced solution allows hotel guests to connect to the network without having to change their IP settings, while still ensuring privacy for each guest. Typically some guests will obtain their IP address from the hotel's DHCP server and others will have statically configured IP addresses in their PCs.</p> <p>The solution is designed to interoperate with a specialised Access Router that is able to deal with the full range of IP addresses that will be in use on the guests' PCs. The Nomadix Access Gateway (from www.nomadix.com) is an example of such a specialised access router.</p> <p>Configuration of the new feature is similar to the existing MAC-forced forwarding configuration. On each edge switch, you also need to enter the following new command before enabling DHCP snooping:</p> <pre>disable dhcpsnooping ipfiltering</pre> <p>You also need to turn on ARP security and allow authorised clients to send only unicast packets, by entering the following commands:</p> <pre>enable dhcpsnooping arpsecurity enable dhcpsnooping strictunicast</pre> <p>This enhancement also introduces the ability to add MACFF servers with static MAC addresses, rather than relying on ARP to determine them based on IP addresses. To do this, enter the command:</p> <pre>add macff server mac=macaddr</pre>	-	-	-	Y	Y	Y	Y	Y	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016662 CR00016891 CR00017335 CR00017937		-	This software release supports the new x900-48FS switch. For an overview of the switch, see “Support for the new x900-48FS switch (CR00016662)” on page 172.	-	-	-	-	-	-	-	-	Y	-	-
CR00016913	PPP	-	This enhancement enables the PPPoE client to establish a session promptly after a restart or power cycle. This is done by sending a PPPoE Active Discovery Terminate (PADT) frame in response to a frame received with an unknown PPPoE session ID.	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00017197	SSH, User, RADIUS	-	SSH sessions to the router or switch can now be authenticated via RADIUS. The router or switch attempts to authenticate an SSH user via RADIUS if the user to be authenticated is not configured in the local user database and the router or switch has RADIUS configured.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017395	Firewall	-	<p>This enhancement enables the firewall to establish accurate MSS (Maximum Segment Size) values for TCP sessions without using the MTU discovery process. MTU discovery depends on ICMP error packets, so does not work in networks that do not forward ICMP error packets.</p> <p>To enable this feature, use the command:</p> <pre>enable firewall policy=name adjusttcpmss</pre> <p>The adjusttcpmss parameter enables the firewall to adjust the MSS value stored inside incoming TCP SYN packets, to reflect the lower of the two MTU values on the ingress and egress interfaces. Normally, for example, if a TCP SYN packet arrives from an interface with an MTU of 1500 and leaves on an interface with an MTU of 1000, the MSS inside the SYN packet will remain at 1460. When this feature is enabled, the MSS will be adjusted to 960 because the firewall knows that the egress interface has a smaller MTU. Note that the firewall does not change the original MSS value if it is already lower than the values of the ingress and egress interfaces.</p> <p>To disable this feature, use the command:</p> <pre>disable firewall policy=name adjusttcpmss</pre> <p>This feature is disabled by default.</p>	Y	Y	Y	Y	Y	Y	-	-	-	-	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017482	IGMP Snooping	-	The IGMP snooping fast leave option has been enhanced, to make it available when multiple clients are attached to a single port on the snooping switch. For configuration information, see “IGMP snooping fast leave in multiple host mode (CR00017482)” on page 173.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017532	WAN Load Balancing	-	WAN load balancing can now also balance traffic across IP interfaces that are configured on VLANs. This means it is now available for the following IP interfaces: <ul style="list-style-type: none"> ■ eth (such as eth0) ■ ppp (such as ppp0) ■ vlan (such as vlan1) 	Y	-	Y	-	-	-	-	-	-	-	-
CR00017701	IGMP	-	IGMP filtering is now available on AT-8600 series switches. For more information, see the <i>IP Multicasting</i> chapter of the switch's Software Reference, or <i>How To Configure IGMP for Multicasting on Routers and Managed Layer 3 Switches</i> , available from www.alliedtelesis.com/resources/literature/howto.aspx .	-	-	-	-	-	-	Y	-	-	-	-

Features in 291-07

Software Maintenance Version 291-07 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-07 for that product series.
- “-” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x0S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017869	IP Gateway	2	If two routes to the same destination were present in a switch, and the route of lower preference was deleted (in other words, the route whose details were present in the hardware routing database), then the hardware routing database was not updated with the remaining route as it should have been. This could cause serious routing issues. This issue has been resolved so that hardware routing database updates are carried out correctly.	-	-	-	-	-	-	-	-	-	Y	Y
CR00018039	Switch	2	Running the command show switch tab=ip could result in a reboot if a large number of routes (10,000 or more) were present on the switch. This issue has been resolved so that the command can run no matter how many routes are present on the switch. However, the output from the command may be truncated due to buffer space restrictions.	-	-	-	-	-	-	-	-	-	Y	Y

Level 3

No level 3 issues

Level 4

No level 4 issues

Enhancements

No enhancements

Features in 291-06

Software Maintenance Version 291-06 provided support for the new Rapier 48w switch. For more information, see [“Support for the new Rapier 48w switch” on page 175](#).

Features in 291-05

Software Maintenance Version 291-05 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-05 for that product series.
- “-” indicates that the issue did not apply to that product series.

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007737	IGMP Snooping	2	When a port left a multicast group, the router or switch assigned the All Groups port to that multicast group. This could be seen in the output of the command show ip igmp —the list of ports for the group would include the All Groups port. This issue has been resolved.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00010003 CR00011533	WAN load balancer, Firewall	2	The router rebooted if a user cleared all active WAN load balancer sessions on a router that had more than approximately 15000 active sessions. This issue has been resolved Also, the maximum session limit for the WAN load balancer should be 2 * the firewall session limit. On AR415S and AR442S routers, users can increase the firewall session limit by adding special feature licenses. Previously, if the firewall session limit changed, it was necessary to reboot the router to update the WAN load balancer session limit. This issue has been resolved. The WAN load balancer limit now updates when you enable the firewall session license.	Y	Y	Y	-	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00012980	VLAN	2	Previously, it was possible to destroy a VLAN when it was configured as an IP interface. This issue has been resolved. Now, you can only destroy a VLAN if it has no IP configuration.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00013041	IPsec	2	The router or switch would establish IPsec Security Associations (SAs) if ISAKMP was enabled but IPsec was disabled. This issue has been resolved. The router or switch only sets up SAs if IPsec is enabled.	Y	Y	Y	Y	Y	-	-	-	-	-
CR00013500	User, 802.1x	2	If the reauthentication period for 802.1x port authentication was set to less than 20 seconds, the router or switch sometimes rebooted. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013527	OSPF	2	When the router or switch produced an OSPF type 7 LSA, it sometimes specified a route out of an interface that was down. This would stop the router or switch from forwarding traffic to the route's destination. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014344	GUI	2	Previously, some GUI pages did not display correctly in version 7 of Internet Explorer. This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-
CR00014851	SHDSL	2	Very occasionally, an AR442S router would reboot if SHDSL interface train-up took an excessively long time. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-
CR00014955	OSPF	2	The router or switch sometimes rebooted when converting OSPF type 7 LSAs to type 5 LSAs. This issue has been resolved by increasing the robustness of the translation mechanism. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015569	Firewall	2	When only NAT was enabled on the firewall, during some TCP connections in which either end of the connection sends FIN (finished) messages immediately after sending some data and the other end ACKs (acknowledges) the data and the FIN message consecutively, the firewall sometimes incorrectly interpreted the first ACK message (intended for the data) as belonging to the FIN message and prematurely shut the connection down. This could prevent the firewall from opening up new connections using the same port numbers. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00015592	BGP, IP Gateway	2	When BGP learned new best routes for a particular destination, it did not always clear any active IP flows that used the previous best route. Therefore, the router or switch continued to forward traffic sub-optimally. This issue has been resolved. Now, when BGP inserts new routes into the IP route table, it deletes all active route flows, so any active flows change to using the new route. The time taken to delete a full table of IP flows has also been greatly reduced.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015736	Switch	2	Sometimes IP routed traffic would be sent out the correct port, but with the destination MAC of another device on the network. This issue was most likely to occur in configurations that use multi-homed interfaces on multiple VLANs for end devices. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00015822	Switch	2	When the command enable ip macdisparity was used, and a static ARP entry was configured with an L2 multicast MAC address, the switch should have broadcast traffic to that multicast MAC address out all ports in the VLAN. This was not happening. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00015861	VRRP	2	After manually disabling the master VRRP router, sometimes a backup router that should assume master status would not do so, and VRRP would cease to function properly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015938	DHCPv6	2	For DHCPv6, the router or switch now supports Prefix Delegation according to RFC 3633. The previous implementation was according to an Internet draft and did not interoperate with other DHCPv6 implementations. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015974	DHCPv6	2	The DHCPv6 client regularly wrote the file client6.dhc, which over time caused unnecessary Flash compactions. This issue has been resolved. The DHCPv6 client now only writes the file when the contents are different from the previous time that the file was written. This greatly reduces the number of Flash compactions caused.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015984	DHCPv6	2	DHCPv6 authentication did not work correctly. This issue has been resolved. You can now configure the router or switch to authenticate DHCPv6 exchanges.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015989	TPAD	2	When using the TPAD autodial feature and sending multiple transactions over a TCP/IP connection, the router or switch responded to good APACS packets by sending an ACK. This ACK was unnecessary and could cause interoperability issues. This issue has been resolved. The router or switch no longer sends the ACK in these circumstances.	Y	Y	Y	Y	-	-	-	-	-	-
CR00016034	IP Gateway, Firewall	2	Previously it was not possible to add a static ARP entry for the corresponding partner address of a /31 subnet interface. This issue has been resolved. The router or switch will now also allow /31 ARP requests to pass through the firewall.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00016060	IGMP	2	If a port was disabled from being an All Routers group port for IGMP, and that port received All Routers group traffic, it would incorrectly be added to the All Routers group. This issue has been resolved.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016128	IPsec, IPv6	2	When the icmptype parameter was changed to none for an IPv6 IPsec policy, an incorrect ICMP type value was displayed in output of the command show config dyn and saved in the configuration file produced by the command create config . This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	-
CR00016180	GUI, Firewall	2	When configuring the firewall with the GUI, the Policy options tab did not update its display when options were changed from the default settings. For example, if the user cleared a checkbox and clicked the Apply button, the router correctly turned off that option, but the GUI showed a check in the checkbox. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-
CR00016200	Core	2	The router or switch's handling of soft errors has been further improved. Soft errors are spontaneous changes in the information stored in a digital circuit, caused by physical effects.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016288	SYN	2	The polarity of the CD output of RS-232 DCE and V.35 DCE SYN cables was reversed—it was ON when OFF was selected and vice-versa. This issue affected AR750S, AR770S, and AR44xS series routers. This issue has been resolved.	Y	-	Y	-	-	-	-	-	-	-
CR00016303	Load	2	The upload command did not always work if the server parameter was set with the set load command instead of being specified in the upload command. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016327	IP Gateway	2	If a policy filter was configured, ping sometimes failed. This happened because the router or switch assigned the ICMP echo replies to an IP flow without checking that the interface for the echo replies matched the interface for the flow. Therefore, the router or switch could use the wrong flow to forward the replies. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016364	DHCPv6	2	If an IPv6 DHCP client was forced to rebind to a router or switch acting as a DHCP server, the server returned incorrect timing parameters to the client. Some clients were able to cope with this, but others could end up losing their DHCP lease. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016365	DHCPv6	2	The following issues occurred with DHCPv6: <ul style="list-style-type: none"> ■ The option IDs for DNS name server and domain search list were incorrect. This caused interoperability issues with other implementations. ■ The domain names specified in the domain name option were encoded incorrectly. This caused interoperability issues with other implementations. ■ If a user entered two DNS servers for a DHCPv6 policy, then saved the configuration, the command was not saved correctly. When the router or switch ran the configuration on start-up, it added only the second DNS server to the policy. These issues have been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016379	IGMP Proxy, Switch, IP Gateway	2	If IGMP proxy was enabled and multicast data was received on a downstream VLAN interface, that data would be transmitted to other interfaces. Also, the VLAN interface that received the data would forward two copies of the packet to other ports on that VLAN. These issues have been resolved.	Y	-	Y	Y	Y	Y	Y	Y	Y	-
CR00016394	IP Gateway	2	ARP did not work correctly on logical /31 interfaces, which prevented regular IPv4 communications from working over these logical /31 interfaces. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016418	STP	2	If the switch received IGMP packets on the non-lead port of a trunk group which was participating in a Spanning Tree, in some circumstances the switch would forward the packets out of an STP-blocked port in the trunk. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016489	BGP	2	When BGP capability matching was changed to strict , that setting was not displayed in output of the command show config dyn or saved in the configuration file produced by the command create config . When the router or switch ran the configuration file on start-up, the capability matching setting reverted to the default of loose . This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016526	PPP	2	An interoperability issue with a malfunctioning PPP peer meant that the peer could ACK an IP address of 0.0.0.0 when it was required to offer a valid public IP address. This issue has been resolved. The router or switch now refuses to accept this incorrect negotiation and instead resends a configure request for an IP address.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016576	IPv6	2	The router or switch sometimes rebooted after receiving an IPv6 router advertisement, or after the command set ipv6 interface was entered. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016621	Switch	2	On 48-port switches, hardware filters with the eport parameter specified did not always behave correctly. This issue has been resolved.	-	-	-	Y	Y	Y	Y	-	-	-
CR00016698	BGP	2	The following issues occurred when using BGP aggregate specifications (created using the command add bgp aggregate): ■ When an aggregate route was originated from routes learnt from external peers, and then all of the contributing child routes were withdrawn by the external peers, the aggregate route was not removed from the routing table. It could still be advertised to external peers. ■ When a network or import entry (add bgp network or add bgp import) resulted in a route entry that had the same prefix length as the aggregate specification, then BGP (correctly) originated the aggregate route. However, deleting the network or import definition did not remove the aggregate route from the routing table. These issues have been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016727	TCP, Telnet	2	The speed of the output from the Telnet server has been increased.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016762	ISDN	2	For AR44xS series routers with system territory set to USA, the ISDN Q.931 SPIDs failed to initialize to the ISDN exchange/ISDN USA profile simulator (both manual and auto SPIDs) after a reboot. This happened because the router did not write *.spd files to Flash memory, so the SPID initialization failed on reboot because the SPIDs did not exist. This issue has been resolved. The *.spd files are now correctly written to Flash memory, which allows SPIDs to initialise after a reboot.	Y	-	-	-	-	-	-	-	-	-
CR00016804	Bridge	2	If an Ethernet packet, including its FCS (Frame Check Sequence), was encapsulated in PPP and bridged to a VLAN interface, the packet could contain two FCS values. This issue has been resolved.	Y	Y	Y	-	-	-	-	-	-	-
CR00016855	Frame Relay	2	When the MTU of a Frame Relay logical interface was modified (by using the command set interface=fr-int mtu=value), incorrect interface and MTU settings were displayed in output of the command show config dyn and were saved in the configuration file produced by the command create config .	Y	Y	Y	Y	-	-	-	-	-	-
CR00016856	Firewall	2	When the firewall policy for an interface had a NAT type of ENAPT, the firewall did not correctly translate the destination addresses of incoming packets that matched "allow" rules. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	-	-	Y
CR00016911	Classifier	2	When a non-default protocol was specified for a classifier, in some circumstances that protocol setting was not displayed in output of the command show config dyn or saved in the configuration file produced by the command create config . When the router or switch ran the resulting configuration file on start-up, the protocol setting was lost. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016940	Core	2	Some versions of the AT-G8T GBIC prevented the switch from detecting and setting up the AT-A47 expansion board correctly. This issue occurred on start-up when the GBIC was installed and had a link up. This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016941	IP Gateway	2	When there were multiple routes to a destination and the best route was deleted from the switch's hardware routing table, the switch did not use the alternative route. Also, the switch only used the best route, even if ECMP was supported. This issue has been resolved. When multiple routes exist and the best route is deleted from the hardware table, the switch now adds the next best route to the hardware table correctly. If the switch supports ECMP, all routes are now added to hardware, not just the best route.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00017006	Switch	2	Previously, the link to the AT-G8T GBIC would not come up automatically when its auto-negotiation slide switch was set to "on". This was because the switch configured the GBIC in a fixed speed mode by default. This issue has been resolved. The link now comes up automatically when the auto-negotiation slide switch is set to "on". To bring the link up when auto-negotiation is set to "off", use the command: set swi port= <i>port-list</i> speed=1000mf	-	-	-	-	-	-	-	-	-	Y
CR00017031	IGMP Snooping	2	If a port on the router or switch joined and left many IP multicast groups, the router or switch sometimes did not transmit all multicast packets to all receivers. This issue has been resolved.	Y	-	Y	Y	Y	Y	Y	Y	Y	Y
CR00017036	Switch	2	In some trunk configurations, the STP state of trunks was incorrectly applied to non-trunk ports. This could result in incorrect traffic flows in the network. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017074	DHCPv6	2	<p>DHCPv6 prefix delegation contained the followed issues:</p> <ul style="list-style-type: none"> ■ previously, the command create dhcp6 range accepted ranges with an invalid prefix length. This issue has been resolved. The router or switch now displays an error unless the prefix length is in the range 48-64. ■ previously, when the router or switch requested a prefix to delegate to its appint interfaces, it could only use prefixes of length 48 or 64. This issue has been resolved. The requesting router or switch can now use any prefix that has been delegated to it, as long as the prefix length is less than or equal to 64 bits. ■ The requesting router or switch would allocate an address to the interface through which it connects to the delegating router or switch. This issue has been resolved. The router or switch no longer does this. 	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00017076	IPsec	2	<p>When entering the command set ipsec policy, the value of the respondsetbadspi was incorrectly reset to its default of false, unless it was also included in the set command. This issue has been resolved.</p>	Y	Y	Y	Y	Y	-	-	-	-	-
CR00017146	IP Gateway	2	<p>When the router or switch's Local address was pinged, the router or switch responded from the interface address of the interface through which it received the ping, instead of the Local address to which the ping was sent. This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00017151	Telnet	2	<p>When Reverse Telnet was enabled the command shell was (correctly) disabled on all ASYN ports apart from ASYN0. However when Reverse Telnet was disabled again, the command shell was not re-enabled on the other ASYN ports. This issue has been resolved.</p>	Y	Y	Y	Y	-	-	-	-	-	-
CR00017239	VLAN, IGMP Snooping	2	<p>When a user configured IGMP static router ports, the configuration file produced by the command create config could be invalid. When the router or switch ran the resulting configuration file on start-up, it produced an error instead of configuring the router ports. This issue has been resolved.</p>	Y	-	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00017257	WAN Load Balancer	2	<p>If two WAN load balancer healthcheck hosts were defined, and one was unreachable and the other was reachable, WAN load balancer resources were (correctly) in the UP state because at least one healthcheck host was reachable. However, removing the reachable host (by using the command delete wanlb healthcheck) should have changed the WAN load balancer resources to the DOWN state, but did not.</p> <p>This issue has been resolved. If the only healthcheck host available is unreachable and the resource is currently in the UP state, the next unreachable healthcheck received from that host now forces the resource to the DOWN state.</p>	Y	Y	Y	-	-	-	-	-	-	-

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00008225	Core	3	<p>Some early software versions, on some products, supported the command show system temperature. This command was deprecated after version 2.6.4. If a user entered this command on any product, the following message was displayed:</p> <p>Info (1034107): SHOW SYSTEM TEMPERATURE is no longer available. Please use SHOW SYSTEM ENVIRONMENTAL instead.</p> <p>However, only the following products use the show system environmental command to display the temperature: AR750S and AR770S routers, and AT-8600, AT-8800, AT-8948, x900-48, and AT-9900 series switches.</p> <p>Other products use show system instead. On the other products, the above error message was incorrect because it stated that the show system environmental command was available.</p> <p>This issue has been resolved. On products that do not use show system environmental, the following error message is displayed if you enter the show system temperature command:</p> <p>Info (1034090): Command unavailable on this product.</p>	Y	Y	-	Y	-	-	Y	-	-	Y
CR00009036	File	3	<p>If a user tried to copy a small file (less than 32 bytes) in Flash when there was not enough free Flash space for the file and its header, the router or switch did not generate an error message, and the copying could appear to have succeeded.</p> <p>This issue has been resolved. The error message:</p> <p>Insufficient space to store file [file name]</p> <p>is now displayed under those conditions.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00010518 CR00010710	Core	3	<p>The show cpu statistics were unnecessarily inaccurate. For example, a router or switch that was effectively idle showed a CPU usage of 10% to 12%.</p> <p>This issue has been resolved. When the router or switch is effectively idle, the CPU usage now displays as less than 5%.</p>	-	Y	-	-	-	-	-	-	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00011629	PIM, PIM6, ECMP	3	Previously, the switch's count of PIM4 and PIM6 bad Bootstrap Messages (BSMs) could be high, because the switch forwarded BSMs over interfaces that contained an Equal Cost Multipath (ECMP) route to the receiving interface. This issue has been resolved. BSMs are no longer forwarded via all interfaces contained in an ECMP group, but only via one interface in the group.	-	-	-	-	-	-	-	Y	Y	-
CR00012495	IGMP	3	When an IGMP filter was destroyed, switch ports that used the filter did not have their IGMP filter setting returned to "None". This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014324	PPP	3	The interface MIB ifInOctets and ifOutOctets counters displayed by the show ppp counter command incorrectly included the lower layer framing octets and were 5 octets per frame greater than they should have been. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00014919	QoS, DHCP snooping	3	DHCP snooping accepted a minimum of one new client per QoS flow group, instead of a minimum of one new client per port. This meant that DHCP snooping sometimes did not respect the lease limit (maxlease) on a port. This issue has been resolved.	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00015092	ATM	3	Previously, the information output by the "?" help for the ATM channel pcr parameter was incorrect. This issue has been resolved. The "?" help now displays: required - decimal in the range 32-155000 (dependant on physical interface) If you enter a value larger than the maximum PCR allowed on a specific physical interface, the router now displays the following message for ADSL: The PCR supplied was too large, the maximum is 1024 and the following message for SHDSL: The PCR supplied was too large, the maximum is 4608	Y	-	-	-	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015558	ASYN	3	Under some circumstances, when a PC terminal emulator was opened to communicate with a router or switch after the router or switch had fully booted up, the login prompt did not immediately display. To display the login prompt, it was necessary to remove and re-insert the cable. This issue applied to all models' ASYN ports except ports on the AR024 PIC. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015690	DHCP6	3	In the command create dhcp6 range , the ip parameter correctly has the syntax <i>prefix1[-prefix2]</i> . However, the second prefix was previously not optional. This issue has been resolved, so that the second prefix (of the form <i>ipv6address/prefixlength</i>) is no longer required. If you do not enter a second prefix, it is now calculated from the first prefix. The second prefix has the same prefix length at the first and has all 1s in the non-significant part of the address. For example, the second prefix for 3ffe:1:2:3::/64 would be 3ffe:1:2:3:ffff:ffff:ffff:ffff/64.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015881	SNMP, Switch	3	The SNMP objects dot3StatsSQETestErrors and dot3StatsCarrierSenseErrors are not supported on AR750S, AR410, and AR450S routers. Previously SNMP GET got a random value for these objects. This issue has been resolved. SNMP GET now gets 0 for these objects.	Y	-	Y	-	-	-	-	-	-	-
CR00015969	WAN load balancer	3	After the command reset wanlb resource=all was entered, WAN load balancer resources would show their state as "UP" even if the underlying IP interface was down. This issue has been resolved.	Y	Y	Y	-	-	-	-	-	-	-
CR00016001	DHCPv6	3	When a DHCPv6 client was soliciting for servers, the selection of the best server did not proceed in the way specified by the RFC. This issue has been resolved.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016177	Switch, MIB	3	The default value of the MIB object ifJackType for the GBIC slot on AT-8800 series switches was incorrect if no GBIC card was plugged in. This issue has been resolved. The default value is now "other(1)".	-	-	-	-	Y	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016228	QoS	3	If a QoS policy uses the same classifier more than once, the router or switch now displays a warning message. You should not use a classifier more than once in a policy because the operation of such policies is unpredictable.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016463	DHCPv6	3	For the command create dhcp6 range , DHCPv6 now checks that the specified address or prefix range is valid for the specified type of range. Valid options are: <ul style="list-style-type: none"> ■ address1-address2 (e.g. 3ffe:1:2:3:4:5::1-3ffe:1:2:3:4:6::ffff) This is a range of addresses for address assignment (type=normal or type=temporary). ■ address/prefixLen (e.g. 3ffe:1:2:3:4:5::/96) This is a range of addresses for address assignment (type=normal or type=temporary). ■ address/prefixLen-address/prefixLen (e.g. 3ffe:1:2::/48-3ffe:1:40::/48) This is a range of prefixes for prefix assignment (type=pd). 	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00016799	Core	3	For revision M1 of AR770S routers, the low-end threshold for monitoring the 1.2 volt rail was too high. This caused power supply monitoring false alarms. To check the router revision, use the command show system and check the “Rev” entry underneath the time and date. This issue has been resolved—the threshold is now correct.	-	-	Y	-	-	-	-	-	-	-
CR00017008	Core	3	Revisions M3-1 and later of the AR745 router do not support Redundant Power Supplies. Therefore, for these routers, RPS monitoring information has been removed from output of the command show system , and it is no longer possible to use the command set sys rpsmonitor .	-	Y	-	-	-	-	-	-	-	-

Level 4

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00000396	IGMP	4	If a static IGMP port went link down, it was not shown in the “Static Ports” list in the output of the show ip igmp command. This was only a display issue. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011560	Install	4	It is no longer possible to specify a compact flash file as the boot configuration file. If the command set config=cf:filename.cfg is entered, the router or switch does not change the current boot configuration file and instead displays the following error message: Cannot specify configuration file in Compact Flash	-	-	Y	-	-	-	-	Y	Y	Y
CR00013976	IGMP	4	The list of parameters output by the “?” help for show ip igmp ? incorrectly included “IGMP”. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015543	Bridge	4	In output of the command show bridge spanning , the bridge identifier was correctly displayed as a hexadecimal number, but it was not obvious that the number was hexadecimal. This issue has been resolved. The output now has 0x in front of the hexadecimal number, to make it clear that it is hexadecimal.	Y	Y	Y	-	-	-	-	-	-	-
CR00016126	QoS, Switch	4	When a QoS policy was associated with a port that was set to a speed less than the maximum speed of the port, a warning message would be displayed on the console session and in the log when the port state changed to UP. This message stated that the QoS policy operation may be affected by the speed setting of the port. Having this message displayed on the console was considered unnecessary and potentially confusing. This issue has been resolved. The message is now only displayed in the log.	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR00016451	IP Gateway	4	When a second metric was displayed in the output of the command show ip route (because of OSPF, for example) this metric was truncated to 2 characters. This issue has been resolved. The output now displays both metrics in a field up to 10 characters long.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014288	GUI	-	An ADSL connection option has been added to the Wizards page of the GUI for AR44xS routers. This option links to the xDSL configuration section, which lets you configure all basic ADSL or SHDSL settings on one convenient page. If your router GUI does not open at the Wizards page, click on the Wizards button at the top of the left-hand menu to access it.	Y	-	-	-	-	-	-	-	-	-
CR00014667	PPP	-	This enhancement increases the amount of time that the router or switch waits for a CHAP Success message. This enables the router or switch to successfully complete authentication, even in particularly slow networks. The first authentication attempt still times out after 3 seconds, but the second attempt takes 6 seconds to time out, and any further attempts take 9 seconds.	Y	Y	Y	Y	Y	-	-	Y	Y	Y
CR00015432	ADSL, GUI	-	The GUI for AR440S and AR441S routers now displays statistics for the ADSL port. You can now see: <ul style="list-style-type: none">■ a pop-up summary box, by clicking on the port on the System Status page■ ADSL port details, by selecting the new ADSL Statistics page in the Diagnostics menu■ ADSL port counters, by selecting the new ADSL Counters page under Layer 1 Counters in the Diagnostics menu	Y	-	-	-	-	-	-	-	-	-
CR00016078	Software QoS, PPP, Ethernet, VoIP	-	The router or switch now supports software QoS on PPPoE interfaces. Note that this enhancement is not available on AR770S routers.	Y	Y	Y	Y	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016150	IPsec, IPv6	-	<p>To establish a tunnelled IPsec connection for IPv6, you may need to specify the source IP interface in the IPsec and ISAKMP policies. This enhancement enables you to do so.</p> <p>To specify the source interface, use the srcinterface parameter in the commands:</p> <pre>create ipsec policy=name <other parameters> set ipsec policy=name <other parameters> create isakmp policy=name <other parameters> set isakmp policy=name <other parameters></pre> <p>The global address of the source interface (if available) will be used as the local address of the policy.</p>	Y	Y	Y	Y	Y	-	-	-	-	-
CR00016221	Load, MIBs	-	<p>With this enhancement, you can use SNMP to:</p> <ul style="list-style-type: none"> ■ set parameters for uploading files from the router or switch, and ■ upload files to a TFTP server <p>SNMP already lets you save the current configuration to a file on the router or switch. You can use this with the new options to back up the configuration to a TFTP server.</p> <p>For more information, see “Backing up the configuration with SNMP (CR00016221)” on page 176.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016234	DHCP Snooping	-	<p>This enhancement enables the router or switch to log discarded ARP requests when ARP security is enabled. By default, discarded ARP requests are not logged. To turn logging on, use the command:</p> <pre>enable dhcpsnooping log=arpsecurity</pre> <p>To turn it off, use the command:</p> <pre>disable dhcpsnooping log=arpsecurity</pre> <p>To see whether it is enabled, use the existing command:</p> <pre>show dhcpsnooping</pre> <p>and check the new "Logging enabled" entry.</p> <p>To view the log entries, use the command:</p> <pre>show log</pre>	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00016285	MACFF	-	<p>It is now possible to use MAC-forced forwarding on non-private VLANs. Because MAC-forced forwarding is primarily a security feature, the switch displays a warning message if you do so.</p> <p>This enhancement allows you to use MAC-forced forwarding to limit broadcast traffic in a network where private VLANs are not appropriate.</p>	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00016361	Switch	-	AT-8948, AT-9900 and x900-48 series switches now support AT-SPTX tri-speed Cu SFPs.	-	-	-	-	-	-	-	Y	Y	-
CR00016437	MSTP	-	In the command set mstp configname=name , the switch now accepts the character "." in the name .	-	-	-	Y	Y	Y	Y	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016459	Core	-	<p>This enhancement disables CPU fan monitoring on AT-8948 switches. Monitoring the fan is unnecessary unless an accelerator card is installed on the switch, so disabling monitoring reduces the number of messages that the switch displays and logs.</p> <p>To enable monitoring, use the command:</p> <pre>enable cpufanmonitoring</pre> <p>To disable it again, use the command:</p> <pre>disable cpufanmonitoring</pre> <p>When monitoring is enabled, the command show system displays the CPU fan status in the entry labelled "Main fan".</p>	-	-	-	-	-	-	-	Y	-	-
CR00016523	SNMP	-	<p>This enhancement enables you to specify whether SNMP adds 0x00 padding when the most significant 9 bits of an object's value are all 1, or whether the encoding follows the ASN.01 BER rule, which cuts off the most significant byte of 0xff. This setting has an impact on all integer type MIB objects, including 32 bit and 64 bit counter objects.</p> <p>To add the padding, use the command:</p> <pre>set snmp asnberpadding={only yes true}</pre> <p>For examples, see "SNMP ASN.01 BER Padding (CR00016523)" on page 179.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00016758	IP NAT	-	<p>This enhancement enables you to turn off TCP state and sequence checking in IP NAT. It also allows all ICMP packets go through IP NAT.</p> <p>To do this, use the command:</p> <pre>enable ip nat bypasstcp</pre> <p>When bypasstcp is enabled, IP NAT performs IP address and port translation for TCP packets and forwards the packets, regardless of the TCP sequence number and the current TCP state. It also allows ICMP echo reply and other ICMP packets to initiate a session and get forwarded.</p> <p>To disable the bypassing, use the command:</p> <pre>disable ip nat bypasstcp</pre> <p>Bypassing is disabled by default because it degrades the security of IP NAT. However, it is useful when you need NAT on VRRP routers.</p> <p>Note that this enhancement does not apply to firewall NAT.</p>	Y	Y	Y	-	-	-	-	-	-	-
CR00016776	IP Gateway	-	<p>This enhancement allows ARPs to move between ports on the router's VLAN interfaces. This assists with wireless station roaming.</p> <p>To enable this feature, use the command:</p> <pre>enable ip arp silentroam</pre> <p>To disable it, use the command:</p> <pre>disable ip arp silentroam</pre>	Y	-	Y	-	-	-	-	-	-	-
CR00016785	Core	-	<p>The default summertime dates have been updated to reflect the changes for North America made by the American Energy Policy Act of 2005.</p> <p>By default, summertime now starts on the second Sunday in March and ends on the first Sunday in November.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00016977	Script	-	<p>This enhancement enables you to use aliases in commands in script files. The router or switch expands the aliases when it runs the script (except when it runs the script at start-up).</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Features in 291-04

Software Maintenance Version 291-04 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” indicates that the resolution is available in Version 291-04 for that product series.
- “–” indicates that the issue did not apply to that product series.

Level 1

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013787	ISAKMP, Logging	1	It was possible for invalid log messages to overwrite the log message buffer and cause the router or switch to reboot. Such invalid log messages could occur with VPN tunnels, for example. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013813	TTY, User	1	When a user telnets into the router or switch, to login via RADIUS authentication, the telnet connection establishes and then user login authentication starts. Previously, if the remote user closed the telnet connection before RADIUS responded to the authentication request, then the router or switch rebooted when it received the RADIUS Reply message. This issue has been resolved. The router or switch now does not reboot if the telnet connection is closed before the RADIUS Reply message arrives.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013963	Switch	1	Under heavy broadcast traffic, it was possible for the switch forwarding database (FDB) to lock up. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014145	Core DHCP Snooping	1	DHCP Snooping determines when a client lease will expire by taking the current time and adding the client's assigned lease period to it. Previously, DHCP Snooping did not update this expiry time if the switch's clock time changed, which can happen because of NTP, summertime, or a user manually re-setting the time. Therefore, if the switch's clock time changed, DHCP clients could expire and lose connectivity. This issue has been resolved. If the switch's clock changes, DHCP Snooping now updates its client expiry times.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00016314	Core	1	AR442S routers did not run the user-specified configuration script at start up. Also, they incorrectly displayed the message “INFO: Initialising Flash File System” twice during start up. These issues have been resolved.	Y	–	–	–	–	–	–	–	–	–

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010511	BGP	2	Turning defaultoriginate on or off for a BGP peer (by using the command add bgp peer) did not cause BGP to generate an update, even if automatic updating was enabled (enable bgp autosoftupdate). This issue has been resolved.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00012564	L2TP	2	Setting a timeout on L2TP packet debugging caused the router or switch to reboot. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013592	HTTP	2	A badly formed response from a particular HTTP server caused the router or switch to reboot when it attempted to load a non-existent file from that server. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013700	IP Gateway	2	When an IP packet was queued by the ENCO module or other applications, and the IP flow for the packet became invalid while the packet was queued, the router or switch sometimes rebooted. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013791	IGMP, VLAN	2	Disabling IGMP snooping correctly increased the number of L3 filter matches available. However, if the configuration was saved and then run after a reboot, the switch incorrectly limited the number of L3 filter matches to the number available when IGMP snooping was enabled. If the maximum number of matches had been configured, this meant that some matches were missing after a reboot. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–
CR00013823	Switch	2	In very rare circumstances, a port could stop transmitting traffic if its speed was modified or it was reset while under heavy traffic load. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y
CR00013929	ADSL ATM Ethernet	2	When performing RFC 1483 encapsulation of Ethernet frames, the AR44xS routers did not pad frames out to the 64-byte minimum frame size (the RFC does not require such padding to be performed). This resulted in an interoperability issue with ATM switches that discarded (rather than padded) the undersize frames upon decapsulating them. The effect of this was that when an AR44xS router was connected to an ATM network that contained such switches, the router could fail to connect at the PPP session level. This issue has been resolved. The router now always pads undersize Ethernet frames to the 64-byte minimum frame size before it performs RFC 1483 encapsulation. This avoids the possibility of this interoperability issue.	Y	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014228	Switch	2	When the router generated packets (such as ARP requests) and sent them out multiple LAN ports, it always sent them as untagged packets. This issue has been resolved, so that LAN traffic will be tagged or untagged as specified in the VLAN port configuration.	–	–	Y	–	–	–	–	–	–	–
CR00014269	Switch	2	If a user explicitly set the learn limit to zero by entering the command: set switch port= <i>number</i> learn=0 intrusion=discard and the learn limit had either not been explicitly set previously or had been explicitly set to a non-zero value, then the switch would not learn any MAC addresses. It treated 0 as meaning “learn 0 addresses” instead of meaning “no limit”. This issue has been resolved. A learn limit of 0 means “no limit” in all circumstances.	–	–	–	–	–	–	–	Y	Y	–
CR00014298	Switch	2	Packet loss sometimes occurred when an IGMP snooping group timed out. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–
CR00014323	Switch EPSR	2	When EPSR was used in a network with a 10Mbps multicast or broadcast flow, the EPSR ring frequently alternated between a state of failed and complete. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–
CR00014340	Bridge, Switch, VLAN	2	Bridging STP did not work if a VLAN was added as a bridge port. This issue has been resolved.	Y	–	Y	–	–	–	–	–	–	–
CR00014437	Core Install Stacking	2	If a switch's configuration was saved (by using the command create config=filename), and then the command set config=filename was entered, the configuration file should have been propagated through the stack to other switches that did not have a file of that name. This did not happen. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00014673	Load	2	Attempts to upload a file to a TFTP server failed if a invalid IP address was specified in previous attempts. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014714	PIM	2	If a PIM interface was set as the BSR candidate interface (by using the command add pim bsr candidate interface=interface) and that interface went down, PIM would select another interface as the BSR candidate interface. The router or switch also set the new interface as the BSR candidate interface in the dynamic configuration. This issue has been resolved. PIM only looks for a new interface to use as the BSR candidate address if the user has not specified an interface.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00014748	Reverse Telnet	2	Reverse Telnet used to filter out Ctrl-D characters, making it impossible to perform certain actions on the remote device. This issue has been resolved.	Y	Y	Y	Y	–	–	–	–	–	–
CR00014795	RIPv6	2	When a user disabled RIPv6 or deleted a RIPv6 interface, the router or switch correctly set the metric of any affected RIPv6 routes to 16, indicating that the route was unavailable. However, the router or switch continued to try to use such routes to route packets if no alternative better routes existed. This issue has been resolved. When a route's metric is 16, it is no longer used to route traffic.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00014834	Switch	2	When STP detected a topology change and therefore the switch flushed its ARP table entries, sometimes the switch did not remove entries for non-lead trunk ports. Therefore, ARP entries for these ports contained incorrect routing information. These incorrect entries were not replaced until after they timed out. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y
CR00014925	IP Gateway	2	When the switch had a static route to a destination, and a user added a more specific static route to the same destination, then the switch should have removed the less specific route from its hardware switching table, but did not. This stopped the switch from routing packets to that destination. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014987	Core Switch	2	If a terminal emulator started up after the router started up, the router did not display a login or command prompt. This issue occurred with some terminal emulators (including Tera Term Pro) when connecting to the AR415S router. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–
CR00015032	PKI	2	When adding a certificate to PKI, if the length of the public key in the certificate was longer than 2048 bits (256 bytes) the router or switch could reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015071	IP Gateway	2	Routing over a PPP interface could fail if the switch had a default route out an Ethernet port. The default route switched all packets, even those destined for the PPP interface. This issue has been resolved. The resolution involves adding routes over the PPP interface to the switch hardware tables with an instruction to trap these packets to the CPU. Therefore these routes now appear in the hardware tables, and can be displayed by using the command show switch table=ip .	–	–	–	–	–	–	–	Y	Y	Y
CR00015087	Classifier, DHCP snooping, Switch, MACFF	2	When MAC-forced forwarding (MACFF) was running, the switch did not filter multicast packets correctly. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–
CR00015156	Switch	2	On AR750S, AR750S-DP, and AR400 Series routers, if a user set a switch port to autonegotiate speed and duplex mode (by using the command set switch port=number speed=auto), the link went down. This issue has been resolved.	Y	–	Y	–	–	–	–	–	–	–
CR00015207	Firewall	2	If a VoIP call came in through the SIP ALG from the public side of the firewall and was then transferred by the device on the private side, the firewall session was not always updated. When this happened, the person to whom the call was transferred could not hear the person who had called. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015348	GUI	2	The GUI could not be used to access the dual power supply AR750S-DP router. This issue has been resolved. The GUI resource file to use is 750s_281-06_en_d.rsc.	–	–	Y	–	–	–	–	–	–	–
CR00015396	IP Gateway	2	If you defined an IP filter without specifying the optional type parameter, the default value of type=traffic was added to the filter in the dynamic configuration. This prevented you from using the configuration file with software version 2.7.6 and older releases. This issue has been resolved. The type parameter is only added to the dynamic configuration if you enter a value for it.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015474	Ethernet	2	If an AR020 PRI E1/T1 PIC was installed on an AR415S, the router's Ethernet interface stopped receiving unicast or multicast packets correctly—it only received broadcasts correctly. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–
CR00015638	Switch	2	On AR770S routers, when generating multicast or broadcast CPU traffic out a VLAN that had multiple active switch ports in it, the traffic would only egress port 1. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–
CR00015697	Switch	2	Mirroring the traffic on port 1 of any line card caused the switch to lose packets.	–	–	–	–	–	–	–	–	–	–
CR00015925	ADSL	2	The ADSL Annex B firmware has been updated on AR441S routers. This improved interoperability with some DSLAMs.	Y	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015936	Switch	2	<p>It was not possible to set a tri-speed SFP to a fixed speed in the configuration script that the AT-9924SP switch runs when it starts up.</p> <p>This issue has been resolved, so the SFP can be set to a fixed speed from the configuration script</p> <p>Also, it was possible to use the command set swi port=number speed on an empty SFP bay. The command reported that the operation had been successful, but an inserted SFP was instead set to its previous or default setting.</p> <p>This issue has been resolved. It is no longer possible to set the speed of an empty SFP bay.</p>	–	–	–	–	–	–	–	–	Y	–
CR00015949	IPv6	2	<p>Sometimes, when a router or switch received an IPv6 router advertisement message, it incorrectly created a duplicate of an already-existing interface route. If a user then deleted the IPv6 interface that these two routes belonged to, the router or switch could reboot.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00015971 CR00015937 CR00015864	WAN Load Balancing	2	<p>The following issues occurred with WAN load balancing (WANLB):</p> <ul style="list-style-type: none"> ■ when a WANLB resource port became unavailable, existing sessions on the unavailable resource did not move to a backup resource ■ if packets were sent over a WANLB session, then that session timed out, and then the same packets were sent again, a new session did not establish. This stopped the packets from being sent the second time. ■ when WANLB was used with Firewall NAT, the orphan timeout setting of WANLB sessions was not updated correctly. This could mean that WANLB resources appeared to be available when they were not. <p>These issues have been resolved.</p>	Y	Y	Y	–	–	–	–	–	–	–
CR00016037	User	2	<p>If the router or switch used RADIUS authentication and all the RADIUS servers were unavailable, then the device correctly checked its user database for a RADIUS backup user and authenticated that user. However, if that user then logged out, they were unable to log in again until after the RADIUS server Dead Time timer had expired.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00007000	GUI, IGMP	3	The graphical user interface (GUI) listed an invalid local interface in the Interface drop-down list on the page for adding a static IGMP association. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y
CR00009274	Switch IP Gateway	3	If many VLANs simultaneously went from up to down, or down to up, the switch became unresponsive for a period of time. This issue has been improved by reducing the processing overhead for VLAN state changes.	–	–	–	–	–	–	–	Y	Y	–
CR00009302	Switch	3	The number of filters that can be created on an AT-8848 switch is limited by the number of filter matches available. Previously, if a user attempted to create a filter, and an existing filter already used the same filter match as the new filter, the switch counted this as two matches being used. This reduced the number of available filters. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–
CR00009478	BGP	3	When a peer's inroutemap filter assigned an incoming route to a well-known BGP community, the router or switch did not use the community's restricted advertisement settings, such as NoExport or NoAdvertise. This issue has been resolved. Also, output of the command show bgp peer now shows whether a route has been assigned to a community. This is indicated by a flag “m”, as shown in bold in the following route entry example: <pre>> 192.2.2.0/24 192.168.1.2 IGP - 100 m SEQ 1;</pre> The flag “m” indicates that this route has at least one community attached to it.	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00010136	IP Gateway	3	<p>If an IP interface was added and deleted many times, an excessive number of memory buffers became full.</p> <p>Also, when an IP interface was deleted, the IGMP query timer (set ip igmp int=interface querytimeout=value) sometimes continued running and later caused the router or switch to reboot.</p> <p>These issues have been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012230	IP Gateway	3	<p>When running the boot ROM release, it was possible to configure the router or switch as a DHCP client by using the command add ip interface=int ip=dhcp. However, the boot ROM release does not include the DHCP client feature, so the router or switch did not receive an IP address via DHCP.</p> <p>This issue has been resolved. It is no longer possible to configure the router or switch as a DHCP client when running the boot ROM release.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012493	IP Gateway, IGMP Proxy	3	<p>Where IGMP proxy is enabled, only one upstream interface may be defined. Previously, when the command add ip interface=int ip=ipadd igmpproxy=upstream was used to try to create a second upstream interface, an error message was correctly displayed. However, the interface was still added, using igmpproxy=off.</p> <p>This issue has been resolved. The second interface is no longer added if this error occurs.</p> <p>Also, if an interface had been set as the upstream interface and was later changed to a downstream interface, a different upstream interface could not be specified, even though there was no active upstream interface.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	—

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00012585	User	3	<p>When authenticating users via RADIUS, the number of times that the router or switch attempts to contact the RADIUS server is determined by the Server Retransmit Count (displayed in output of the command show radius). Previously, this count incorrectly included the initial request. For example, a Retransmit Count of 3 meant that up to 3 attempts were made to contact the server.</p> <p>This issue has been resolved, so that the Retransmit Count no longer counts the initial request. For example, a Retransmit Count of 3 now means that up to 4 attempts are made to contact the server.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00012832	BGP	3	<p>When the router or switch had thousands of static routes and BGP static import was periodically turned on and off, BGP used an excessive number of memory buffers. Excessive buffer use could also occur with BGP in other rare circumstances.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00012858	DHCP	3	<p>Previously, it was not possible to have multiple static DHCP entries with the same client ID (MAC address), even if the static entries were for different DHCP ranges.</p> <p>This issue has been resolved. You can now add static DHCP entries for a given MAC address to multiple ranges. Note that you cannot have multiple entries for a given MAC address on the same range.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013150	File	3	<p>If a boot configuration script included a command to delete a file followed by a command to create a file of the same name, a fatal exception occurred when the router or switch ran that script on reboot.</p> <p>This issue has been resolved so that the fatal exception no longer occurs.</p> <p>However, you should avoid putting such file operations into boot configuration scripts. To enhance multi-tasking, the file handler performs file operations in the background. This is not possible when executing a boot configuration script, so the file operations may be queued until after boot-up. In this case, this means that the file deletion will not be finished before the file creation command tries to execute.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013629	IGMP	3	When IGMP fast leave was enabled and the switch received a leave message via a trunk port, the switch only removed the port from the multicast group if the port was the master trunk port. This issue has been resolved. When fast leave is enabled, non-master trunk ports now leave multicast groups as soon as the switch receives a leave message.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00013694	Switch, IP Gateway	3	For layer 3 Jumbo frames, this software version improves initial layer 3 flow setup and handling of flows that exceed the layer 3 MTU mid-flow.	–	–	–	–	–	–	–	–	Y	–
CR00014038	IGMP IP Gateway	3	The IGMP Default Timeout Interval is automatically calculated by IGMP in accordance with RFC 2236, but the following command allows you to over-ride the calculated value: set ip igmp timeout= <i>value</i> Previously, the router or switch sometimes set the interval to the calculated value instead of using the value entered in the command above. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014047	DHCP Snooping	3	Previously, DHCP snooping correctly refused to allocate new DHCP leases once the maxleases value had been exceeded, but it did so by discarding the server's acknowledgement message instead of forwarding it to the client. Therefore, the DHCP server recorded the address as allocated, which meant the IP address range could be exhausted. This issue has been resolved. The server no longer records addresses as allocated once the maxleases value is exceeded.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00014152	Switch	3	On AR415S, AR44xS, AR750S and AR770S routers, when a switch port went down or was reset by using the command reset switch port=number , this deleted the dynamically-learned forwarding entries for all ports. This issue has been resolved. Now entries are only deleted for the port that went down or was specified in the command.	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014163	Firewall	3	When the firewall was performing NAT on UDP video streams and two streams started up at the same time, sometimes one or both streams displayed excessive jitter. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–
CR00014178	Core	3	The following issues occurred with environmental monitoring: ■ on AR750S and AR770S routers, the values reported by the show system command were incorrect for the first few seconds after a cold restart ■ on AR770S routers, the router did not indicate power supply problems through log messages or the system LED These issues have been resolved.	–	–	Y	–	–	–	–	–	–	–
CR00014285	BGP	3	The default setting for BGP capability matching is now loose instead of strict . This matches the requirements of RFC 4271.	Y	Y	Y	Y	Y			Y	Y	Y
CR00014305	Switch	3	On AT-8748XL and Rapier 48i switches, mirroring did not work when: ■ only one (not both) of the uplinks had an expansion module installed and ■ that uplink (port 49 or 50) was the mirror port This issue has been resolved.	–	–	–	Y	–	–	Y	–	–	–
CR00014313	GUI, Log	3	If the user cleared the Queue Output checkbox on the Modify Log Output Definition page of the GUI, it displayed an error instead of making the change. This issue has been resolved. The GUI can now be used to turn off queuing of logging output.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y
CR00014327	MSTP, GUI	3	When using the GUI to configure the MSTP CIST, users had to specify the external and internal port path costs. If these were not specified, the GUI gave an error instead of configuring the CIST. This issue has been resolved. By default, the GUI now specifies “default” for the path costs. This value of “default” leaves the current setting unchanged.	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014328	IP Gateway, Switch	3	If a port had static ARP entries defined for a VLAN, then adding the port to another VLAN made those static ARP entries inactive. Also, deleting a port from a VLAN would delete all static ARP entries that were defined on that port, including entries for other VLANs. Note that this deletion issue did not occur on Rapier i, AT-8800, AT-8700XL, or AT-8600 Series switches. Both of these issues have been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00014652	PIM6	3	If a user changes the PIMv6 BSR candidate priority to the same value as the currently-elected BSR's priority, then the router or switch should be elected as the BSR if its IPv6 address is higher than the currently-elected BSR. This did not happen. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00014659	DHCP	3	On the DHCP server, a user could create two static DHCP entries for the same client in one range. This was only possible if the client had first obtained a dynamic address from the server. This issue has been resolved. It is now impossible to add the same static client twice, even when that client has a pre-existing dynamic entry.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014724	IGMP Snooping	3	When the router or switch received an IGMP Leave message, it did not update IGMP Snooping counters correctly in some circumstances. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00014746	WANLB, IP Gateway	3	It was possible to delete an IP interface that was configured as a WAN load balancer resource. This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014755	BOOTP IP Gateway	3	It was possible to add a BOOTP relay destination using an interface that was not running IP. It was also possible to delete an IP interface even though BOOTP relay destinations were defined for the interface. Both of these situations could allow the router or switch to be mis-configured. This issue has been resolved by adding checks for these situations to the command handlers. It is no longer possible to add a BOOTP relay destination using an interface not in use by IP, and no longer possible to delete an IP interface if BOOTP relay has destinations defined using that interface.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014782	PIMv6	3	The command show pim6 staterefresh sometimes corrupted the terminal display output with random characters. To recover, it was necessary to reset the terminal session. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00014872	GUI	3	The router or switch rebooted if the Opera browser was used to browse to its GUI. This issue has been resolved. However, note that the GUI does not fully support Opera. Some functionality may not be available.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015107	GUI	3	HTTP pipelining did not operate correctly on some web browsers when browsing to the GUI. This made some images very slow to load. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y
CR00015126	IP Gateway	3	For IP filters of type=routing , the first filter entry could not be set to match on the following IP address/mask pair: source=0.0.0.0 smask=255.255.255.255 This IP address/mask pair corresponds to the default route. This issue has been resolved. You can now match on the default route in the first entry of a filter.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015148	IP Gateway DHCP	3	When a router or switch was configured to use DHCP to assign an address on an interface, and then set to have a static address on that interface, the DHCP client in the router or switch would continue to negotiate with the DHCP server. This tied up a DHCP lease. This issue has been resolved. Assigning a static address to an interface will stop the DHCP client from requesting an address from a DHCP server.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015155	Load	3	File upload via the IPv6 version of TFTP was not operating correctly. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00015159	IP Gateway	3	If the router or switch received an IP subnet broadcast packet that was directed to a unicast MAC address, it incorrectly responded with an ICMP unreachable message, unless an appropriate IP helper configuration existed. This issue has been resolved. When there is no IP helper configuration, the behaviour now depends correctly on the setting of the directedbroadcast parameter for the IP interface. If directedbroadcast=on , the packet is sent out as a MAC broadcast. If directedbroadcast=off , the packet is dropped. ICMP unreachable messages are not sent in any case.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015258	IGMP snooping VLAN	3	The command add igmpsnooping vlan=vlan routerport=port adds a static IGMP router port, for a specific VLAN and port pair. Previously, it was possible to remove the port from that VLAN without updating the static router port association. This issue has been resolved. When you remove a static router port from a VLAN, the router or switch now removes that port from the static router port list and updates all layer 2 entries.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00015346	Switch	3	The 64-bit counter type objects in the ifXTable of the Interfaces Group MIB (RFC 2863) returned non-zero values for ports that had never been up. This issue has been resolved.	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015666	IP Gateway	3	Subnet broadcast packets would not be routed correctly when the interface to which the subnet broadcast was destined was an interface on the device, but its link status was down. Even though an alternate route to the destination existed, the device would send the packets incorrectly. This issue has been resolved. When a subnet broadcast is received, it will be correctly forwarded to an alternate route even if the destination interface is down.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00015798 CR00016058	Switch	3	If the switch received a packet on a port and therefore started using MAC-based authentication to authenticate the port, and then received another packet during the authentication process, then occasionally the switch dropped the second packet. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR00015915	Ethernet	3	The AR415S router processed some IP multicast packets incorrectly on its eth0 interface. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–

Level 4

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00004677	Core	4	When the router or switch rebooted, its internal clock lost approximately 1 second. This issue has been resolved. The time loss on reboot has been reduced.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00009087	Core, Utility	4	<p>The following issues occurred with the commands show debug active and disable debug active:</p> <ul style="list-style-type: none"> ■ The command did not adequately warn users if an invalid module number had been entered into the active parameter. <p>This issue has been resolved. The router or switch now displays an error unless the value is between 1 and 142.</p> <ul style="list-style-type: none"> ■ The CLI "?" help description for the active parameter listed an incorrect number range and also listed modules that cannot be manipulated through this command. <p>This issue has been resolved. The "?" help description is now correct.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00011695	QoS	4	<p>The "?" help description for switch commands that accept a value in bytes (or similar units such as kbytes or bytes/s) incorrectly indicated that the units were bps. The commands this issue applied to depend on the switch model, but include commands such as:</p> <pre>create qos trafficclass=<i>value</i> maxburst=? create qos policy=<i>value</i> dtcmaxburst=? set qos red=<i>value</i> start1=? set swi port=<i>value</i> bcl=? set swi dlfl=?</pre> <p>This issue has been resolved. The "?" help description now displays the correct units.</p>	–	–	–	Y	Y	Y	Y	Y	Y	Y
CR00012602	MSTP	4	<p>If the command set mstp cist port=<i>value</i> was entered with no other parameters, the resulting error message ("One or more parameters may be missing") was displayed as an INFO message.</p> <p>This issue has been resolved. The message now displays as an ERROR message.</p>	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00013045	SNMP, Core, TTY	4	<p>The MIB object hrSystemNumUsers displayed the number of login users since the router or switch started up, instead of the number of currently-active login users.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013112	IP Gateway	4	The blackhole parameter of the commands add and set ip route had no “?” help description. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–
CR00013188	LACP	4	Previously, when an attempt to add a port to LACP was unsuccessful, the switch displayed an appropriate warning message followed incorrectly by an “operation successful” message. This issue has been resolved. The switch no longer displays “operation successful” when port addition fails.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00013221	IP Gateway	4	The output of the command show ip route did not contain any spaces between the route tag value and the metric value when the tag value was long. This issue has been resolved by adding the missing spaces. The content and relative position of the values have not changed.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013260	TACPLUS	4	If a user added a TACACS+ server when TACACS+ was not enabled, previously the router or switch displayed a single “info” message that indicated that the module was not enabled, but did not display a message confirming the server addition. However, the router or switch did add the server. This issue has been resolved. TACACS+ is now consistent with other modules—the router or switch displays the following “warning” and “info” messages: Warning (2111049): The TACP module is not enabled. Info (1111003): Operation successful.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013463	Ping	4	Previously, if you used the ? or Tab keys to obtain help about the timeout parameter for the ping command, the resulting help said that the maximum timeout was 65535. However, the correct maximum is 60 seconds. This issue has been resolved. The “?” help now displays the correct range of values.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013589	Install	4	<p>When a router or switch was using a trial licence for release software and the trial period elapsed, the router or switch rebooted without indicating the reason for the reboot.</p> <p>This issue has been resolved. The following error messages now explain why the router or switch is rebooting:</p> <p>ERROR: There are no valid licences available for the current software release.</p> <p>The device will now reboot.</p> <p>ERROR: The trial licence for the current software release has expired.</p> <p>The device will now reboot.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013640	NTP	4	<p>Output of the command show ntp displays a "Host Address" field. This is the address of the interface from which the router or switch sends NTP packets. Previously, if the IP address changed, the "Host Address" field did not change, even though NTP used the new address.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014106	Core	4	<p>If the router or switch runs a configuration file on start-up that contains the command set summertime before the command enable summertime, a log message on start-up says that summertime needs to be enabled. However, summertime is correctly applied to the router or switch.</p> <p>Previously, if you configured summertime then saved the configuration by using the command create config, set summertime came before enable summertime in the resulting configuration file.</p> <p>This issue has been resolved. When you save the configuration, enable summertime now comes before set summertime in the resulting configuration file, so the log message is not produced.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014151	VLAN	4	<p>The following error message:</p> <p>"Error (3089399): Operation not allowed on a .NESTED port."</p> <p>contained an extraneous "." before the word "NESTED".</p> <p>This issue has been resolved. The "." has been removed.</p>	-	-	-	-	-	-	-	Y	Y	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014170	Core	4	The show exception command did not display the correct exception type for watchdog exceptions on AR750S, AR750S-DP, or AR770S routers. This issue has been resolved. The correct exception type is now displayed.	–	–	Y	–	–	–	–	–	–	–
CR00014250	LLDP	4	In output of the command show lldp localdata , the field lldpLocSysDesc gives information about the router or switch model and software version. Previously, this information was sometimes split incorrectly across 3 rows. This issue has been resolved. The information now displays correctly.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014318	DDNS	4	If a user made a configuration change to DDNS (dynamic DNS) when DDNS was not enabled, previously the router displayed a message that indicated that the module was not enabled, but did not display a message confirming the change. However, the router did make the change. This issue has been resolved. DDNS is now consistent with other modules—the router displays the following “warning” and “info” messages: Warning (2142049): The DDNS module is not enabled. Info (1142003): Operation successful.	Y	–	Y	–	–	–	–	–	–	–
CR00014367	GUI	4	The GUI included pages for configuring MAC-based port authentication. However, this feature is not available on AT-9800 Series switches. This issue has been resolved. The GUI pages have been removed.	–	–	–	–	–	–	–	–	–	Y
CR00014712	Firewall	4	If the router or switch renumbered a firewall rule, it displays a message. Previously, this message had a status of “info” instead of “warning”. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00014750	DHCP	4	Previously, when a user entered the command delete dhcp range=range ip=ipadd , the router or switch would display an “Operation successful” message, even when the client entry in question was unused. This issue has been resolved. For unused clients, this command now results in the following new message: “Nothing to delete, client is unused.”	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014778	VLAN, Bridging	4	It was possible to specify a value of 0 for the ageingtimer parameter in the command add and set vlan=vlan bridge , even though this value was meaningless. This issue has been resolved. The lowest valid value for ageingtimer is 1.	Y	–	Y	Y	–	–	–	–	–	–
CR00015080	ATM	4	When an SHDSL or ADSL interface re-trained after having been in a “link up” state, spurious error messages could appear on the console. This issue has been resolved. The messages were not genuine error messages and no longer appear.	Y	–	–	–	–	–	–	–	–	–
CR00015130	Switch	4	The following commands have been deprecated in software versions 2.9.1 and later, and therefore (correctly) have no effect on the switch: set switch port= <i>number</i> thrashlimit= <i>value</i> set switch port= <i>number</i> thrashrefill= <i>value</i> Previously, if a user entered these commands, the switch incorrectly displayed an “Operation successful” message. This issue has been resolved. The switch now displays a warning message indicating that the commands are deprecated. For information about the commands that replace these commands, see the “Limiting Rapid MAC Movement” section of the Switching chapter of the Software Reference.	–	–	–	–	–	–	–	Y	Y	–

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00003036	Core	-	It is now possible to hotswap NSMs on NEBS-compliant Rapier i switches. To hotswap the NSM, press the Hot Swap button beside the NSM, check that the Swap LED turns on and the In Use LED turns off, then remove the NSM. Place the new NSM in the bay, then press the Hot Swap button again to make the NSM available for use.	–	–	–	Y	–	–	–	–	–	–
CR00012881	IP Gateway	-	The IP implementation has been enhanced to accept IP interfaces with a /31 netmask. This results in a slightly non-standard subnet that has no network address or broadcast address. This has become a popular extension to IP, because it reduces wastage of IP addresses on point-to-point links.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013129	Many	-	This enhancement extended the “?” help for VRRP, OSPF, SNMP, IP routes, user database, VLANs, logging, and file management. The “?” help for these (and several other) modules now gives information about all command parameters.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00013449	Firewall	-	The firewall now supports FTP sessions that use the security extensions defined in RFC 2228. Previously, the firewall dropped sessions that used those security extensions. This enhancement makes more-secure FTP available between private-side clients and public-side servers, and between public-side clients and private-side servers.	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00013610	Telnet TTY	-	This enhancement enables you to select whether the system name appears at the login prompt for telnet client sessions. By default, the system name appears. To prevent it from appearing, use the command: SET TELnet LOGINSYSstemname=OFF Note that the login prompt appears before you log into the router or switch.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013992	Core	-	<p>AR770S routers have a CPU fan that the software now monitors in the same manner as the main fan. The state of the CPU fan is displayed along with that of the main (chassis) fan in the output of the show system command.</p> <p>If a problem develops with the CPU fan, the router notifies you in the following ways:</p> <ul style="list-style-type: none"> ■ The system LED flashes in a single flash pattern ■ An SNMP trap is issued on the fanAndPSMainFanStatus atRouter private MIB object ■ A log message is generated that says “CPU fan status is not good”. 	-	-	Y	-	-	-	-	-	-	-
CR00014067	File	-	<p>The commands create file, add file, reset file permanentredirect, and show file permanentredirect were not supported on AR725 and AR745 routers. These commands enable you to save the output of other router commands in text files on the router.</p> <p>For more information about these commands, see the “Managing the File System” chapter of the Software Reference.</p>	-	Y	-	-	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014172	BOOTP	-	<p>This enhancement enables you to associate a BOOTP relay destination with a given interface. To do this, use the new optional interface parameter in the command:</p> <p>ADD BOOTp RELAY=<i>ipadd</i> INTerface=<i>interface</i></p> <p>BOOTP packets received on this interface are relayed to the specified relay destination only. You can define the same interface for multiple relay destinations; the router or switch relays any BOOTP packets received to each relay destination.</p> <p>If you do not specify an interface, the destination becomes a “generic” destination. If the router or switch receives a BOOTP message on an interface for which no specific destination is defined, the router or switch relays the message to all generic destinations. This is the same as the behaviour prior to this enhancement.</p> <p>To remove a destination that is associated with an interface, use the command:</p> <p>DELeTe BOOTp RELAY=<i>ipadd</i> INTerface=<i>interface</i></p> <p>To see the interfaces that each destination is associated with, use the pre-existing command:</p> <p>SHow BOOTp RELAY</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014238	DHCP Snooping	-	<p>DHCP snooping records its client database into a file in NVS (if possible) or Flash memory. In previous versions, that file was named bindings.dsn. From this version, the file structure has changed and the file is now named bind0002.dsn.</p> <p>When you upgrade a switch to this version, the switch creates the new client database file 10 seconds after initialising the new version. After that, you can safely delete the old bindings.dns file, if desired.</p> <p>Note that the functionality of DHCP snooping has not changed, only the filename.</p>	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014241	BGP IP Gateway	-	<p>This enhancement enables you to force BGP to select the best route on the basis of network prefix alone, instead of on the basis of preference, then metric, then network prefix.</p> <p>To do this:</p> <ol style="list-style-type: none"> 1. Give the desired dynamic routing protocol a preference of 0, which is the preference of interface routes, by using the command: SET IP ROUTe PReference=0 PROTOcol={BGP-ext BGP-int OSPF-EXT1 OSPF-EXT2 OSPF-INTER OSPF-INTRa OSPF-Other RIP ALL} 2. Create a route map to give matching routes the same metric as your interface routes. To change the metric, use the command: ADD IP ROUTEMap=<i>routermap</i> ENTry=1..4294967295 SET METRic=1 3. Add the route map as a filter to the BGP peers by using the command: ADD BGP PEer=<i>ipadd</i> REMoteas=1..65534 INRouteMap=<i>routermap</i> [<i>other optional parameters</i>] <p>The above process gives matching routes the same preference and metric as interface routes. This forces IP routing to compare the network prefixes of the interface route and the other routes. IP routing then chooses the most specific route as the best route for that destination, instead of automatically choosing the interface route as the best route without considering any other routes which may have more specific network prefixes.</p>	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014300	DHCP Snooping, MACFF	-	<p>The following enhancements have been made to DHCP snooping, to support MAC-forced forwarding:</p> <ul style="list-style-type: none"> ■ MAC-forced forwarding checks the DHCP snooping database to find out which router has been assigned to each DHCP client. DHCP snooping determines this from the router list in DHCP acknowledgement messages. However, some clients do not request a router. DHCP snooping now modifies request messages from such clients, to ensure that they request a router. This enables MAC-forced forwarding to interoperate with such clients. ■ Output from the command show dhcpsnooping database now displays the list of routers that are assigned to each client, as shown in bold in the following example: <pre> Current valid entries MAC Address IP Address Expires(s) VLAN Port ID Source Router list ----- 00-00-cd-28-06-7b 192.168.99.1 52 1 13 2 Dynamic 192.168.199.254 </pre>	-	-	-	Y	Y	Y	Y	Y	Y	-
CR00014354	Ethernet Switch	-	<p>This enhancement enables you to use 100 Mbps fiber SFPs with AR770S routers. Support has been added for AT-SFPX/15 and AT-SFPX/40 SFPs.</p>	-	-	Y	-	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014715	DNS	-	<p>A new log message has been added to provide more information about rejected DNS requests. The message has a log type of 052 / IPDNS and subtype 002 / UNRES, and reads:</p> <p>DNS request for <domain-name> rejected by server. Code <number>, <explanation>.</p> <p>The following codes and explanations exist:</p> <p>0: No Error—no error occurred</p> <p>1: Format Error—there was a problem with the message construction</p> <p>2: Server Failure—there was a problem with the server itself</p> <p>3: Name Error—the name does not exist in the domain</p> <p>4: Query Not Implemented—the received query was not supported</p> <p>5: Refused—Refused for policy, rather than technical, reasons</p> <p>6: YX Domain—the name exists when it should not</p> <p>7: YX RR Set— a resource record exists that should not exist</p> <p>8: NX RR Set— a resource record that should exist does not exist</p> <p>9: Not Authoritative—the receiving server is not authoritative</p> <p>10: Not Within Zone—the specified name is not within the zone specified in the message</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00014728	DDNS	-	<p>When you activate a Dynamic DNS (DDNS) update (by entering the command activate ddns update), the router now warns you of possible negative consequences and prompts you for whether or not to continue.</p> <p>Also, if you attempt to activate a DDNS update when DDNS is disabled, the router displays a warning message that indicates that DDNS is disabled.</p>	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014845	IP Gateway OSPF	-	<p>When OSPF is running over an on-demand PPP link and the link goes down, IP notifies OSPF that the link is down and OSPF stops sending Hello packets over the link. In a network in which routes over the PPP link are all dynamically learnt through OSPF, the PPP link will not come back up because without OSPF there are no routes to direct traffic at that link.</p> <p>This enhancement enables you to stop IP from notifying OSPF that the PPP link is down. OSPF keeps sending Hello messages, which bring the link back up again.</p> <p>To enable this feature, set the new optional notifyospfdown parameter to no in one of the commands:</p> <pre>ADD IP INTERface=int NOTIfyospfdown={NO YES} [other parameters] SET IP INTERface=int NOTIfyospfdown={NO YES} [other parameters]</pre> <p>The default value for this parameter is yes, which means that IP notifies OSPF when the interface goes down and OSPF sets the interface state to Down. OSPF does not send Hello messages to the interface, and OSPF is inactive on the interface until it receives an Up notification. This is the behaviour prior to this enhancement. Also note the following points:</p> <ul style="list-style-type: none"> ■ the parameter applies to the entire IP interface, not an individual logical interface. Setting it on one logical interface sets it on all other logical interfaces associated with the same IP interface. ■ the parameter only applies to on-demand PPP links. IP always sends notifications for other interfaces, even if this parameter is set to no. <p>To see the parameter setting, use the existing command show ip interface.</p>	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00015269	Switch, EPSR	-	<p>EPSR uses a classifier-based hardware filter to select packets in the control VLAN. The hardware filter now only uses 2 of the available 16 bytes to match packets. This increases the number of other classifier-based features you can use when running EPSR.</p>	–	–	–	–	–	–	–	Y	Y	–
CR00015628	Switch	-	<p>The switch now fully recognises the latest revision of the AT-SPTX SPF, so all of the features of the SFP can be utilised.</p>	–	–	–	–	–	–	–	–	Y	–

Features in 291-03

Software Maintenance Version 291-03 includes the resolved issues and enhancements in the following tables. In the tables, for each product series:

- “Y” in a white column indicates that the resolution is available in Version 291-03 for that product series.
- “-” in a white column indicates that the issue did not apply to that product series.
- a grey-shaded column indicates that Version 291-03 has not been released on that product series.
 “-” in a grey column indicates that the issue did not apply to that product series.
 “Y” in a grey column indicates that the issue applied to that product series. These issues are resolved in the next Version (291-04).

Level 1

No level 1 issues

Level 2

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014960	Switch RIPng	2	Creating a large number of IPv6 RIPng interfaces (more than 250) sometimes caused the switch to reboot. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00015102	IPv6	2	If a large number of IPv6 multicast routes were added (more than 1000) on a switch with an IPv6 accelerator card, the switch could reboot. This issue has been resolved.	-	-	-	-	-	-	-	Y	Y	-
CR00015585	ATM	2	AR442S routers sometimes rebooted while using the Test Facility to test the SHDSL interface. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00015678	IPv6	2	<p>When a switch was heavily loaded with IPv6 traffic, it could reboot because a large quantity of traffic was queued while waiting for a neighbour's MAC address to resolve.</p> <p>This issue has been resolved by limiting the number of packets that can be queued while waiting for a neighbour's MAC address to resolve.</p>	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Level 3

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00013270	QoS	3	<p>By default, queue lengths were set to the maximum possible values for each port type. This could make low-priority queues inappropriately starve higher-priority queues of buffer resource.</p> <p>This issue has been resolved. The default queue length has been reduced to 128 frames for all port types. If required, you can change them by using the existing command:</p> <p>SET QOS POrt={port-list ALL} EGResqueue[=queue-list] [Length=16..3648] [other optional parameters]</p>	–	–	–	–	–	–	–	Y	Y	–
CR00014306	LLDP Switch	3	<p>The switch included a permanent L3 filter to stop CDP (Cisco Discovery Protocol) packets from being forwarded. This made one less L3 filter match available to users.</p> <p>This issue has been resolved. CDP still requires an L3 filter, but the filter is automatically created when CDP is enabled and destroyed when CDP is disabled.</p>	–	–	–	Y	Y	Y	Y	–	–	–

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014959	QoS	3	Destroying a traffic class or flow group also destroyed all classifiers that were associated with that traffic class or flow group. This issue has been resolved. User-created classifiers are no longer destroyed. Automatically-created classifiers are still destroyed, such as classifiers for DHCP snooping.	–	–	–	Y	Y	Y	Y	Y	Y	–
CR00015510	Switch	3	When the switch performed layer 3 routing across a trunk, it did not balance traffic across all ports in the trunk group. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–

Level 4

No level 4 issues.

Enhancements

CR	Module	Level	Description	AR400	AR7x5	AR7x05	Rapier i	AT-8800	AT-8600	AT-8700XL	x900-48	AT-9900	AT-9800
CR00014222	IGMP snooping, Switch, VLAN	-	<p>IGMP snooping learns which ports have routers attached to them, so it can forward relevant IGMP messages out those ports. By default, snooping identifies router ports by looking for ports that receive specific multicast packets (such as IGMP queries, PIM messages, OSPF messages, and RIP messages).</p> <p>In some network configurations, this learning process cannot identify all router ports. For such networks, this enhancement enables you to statically configure particular ports as multicast router ports.</p> <p>To specify the static router ports, use the new command:</p> <pre>add igmpsnooping vlan={vlan-name 1..4094} routerport=port-list</pre> <p>To stop ports from being static router ports, use the new command:</p> <pre>delete igmpsnooping vlan={vlan-name 1..4094} routerport=port-list</pre> <p>To list the static router ports, use the existing command:</p> <pre>show igmpsnooping</pre> <p>and check the new “Static Router Ports” field.</p>	Y	–	Y	Y	Y	Y	Y	Y	Y	Y

Features in 291-02

Version 291-02 was not released.

Features in 291-01

Version 291-01 was not released.

MAC-forced forwarding enhancements (CR00017819)

This enhancement improved MAC-forced forwarding in the following ways:

- The commands **add** and **set macff server** both now allow you to optionally specify a MAC and/or IP address for the static entry. The complete syntax is now:

```
add macff server interface=vlan [description=description] [ipaddress=ipadd] [macaddress=macadd]
set macff server interface=vlan [description=description] [ipaddress=ipadd] [macaddress=macadd]
```
- The IP address is the main identifier in the static entry. It must be unique. You can specify the add command multiple times to specify multiple IP addresses for a single MAC address. It is also possible to have a single IP address resolve itself to duplicate MAC addresses, although not recommended.
- If you specify a MAC address without specifying an IP address, this associates the MAC address with an IP address of 0.0.0.0. You can only associate one MAC address with the IP address 0.0.0.0. The switch will make no attempt to resolve the MAC address.
- If you specify an IP address without specifying a MAC address, the switch attempts to resolve the address by ARPing. If there are multiple MAC addresses for the IP address, the switch uses the first ARP reply.
- If you specify both an IP address and a MAC address, the switch does not attempt to resolve the addresses. Even if it later dynamically learns a different IP address for that MAC address, the static entry takes precedence. However, if the switch learns of a discrepancy, it now produces a log entry. You should investigate the discrepancy—it is likely to be because of a configuration error.
- The command **delete macff server** now allows you to identify the server to delete by entering only its IP address. If the MAC address is not associated with an IP address, you can instead enter only the MAC address.
- Debugging is now on a global basis, not a per-interface basis. Therefore, the commands are now **enable macff debug=options** and **disable macff debug=options**. Also, information about debugging options has been removed from the output of **show macff interface** and instead put in the output of **show macff [counters]**.

IGMP Group MIB (CR00018418)

AlliedWare now includes an IGMP Group MIB. This MIB is available in the file at-igmp.mib.

The IGMP Group has the object identifier prefix igmp ({ modules 139 }), and contains a collection of objects and traps for monitoring IGMP group membership.

The following objects are defined:

- igmpIntInfo ({ igmp 1 }) is a collection of objects for managing IGMP-capable interfaces:
 - igmpInterfaceTable ({ igmpIntInfo 1 }) is a table of IGMP-capable IP interfaces, indexed by interface.
 - igmpIntStatsTable ({ igmpIntInfo 2}) is a table of statistics for IGMP-capable IP interfaces.
- igmpIntMember ({ igmp 9 }) is a collection of objects for managing IGMP group membership:
 - igmpIntGroupTable ({ igmpIntMember 1 }) is a table of IP multicast group memberships.
- igmpSnooping ({ igmp 10 }) is a collection of objects for managing IGMP snooping:
 - igmpSnoopAdminInfo ({ igmpSnooping 1 })
 - igmpSnoopAdminEnabled ({ igmpSnoopAdminInfo(1) 1 }) is a boolean value indicating whether IGMP Snooping is globally enabled.
 - igmpSnoopVlanTable ({ igmpSnooping 2 }) is a table of layer 2 interfaces performing IGMP snooping.
 - igmpSnoopGroupTable ({ igmpSnooping 3 }) is a table of IGMP groups snooped on layer 2 interfaces.
 - igmpSnoopPortTable ({ igmpSnooping 4 }) is a table of ports in layer 2 interfaces that are currently members of multicast groups.
 - igmpSnoopHostTable ({ igmpSnooping 5 }) is a table of hosts receiving multicast data.

ICMP Router Discovery Advertisements (CR00010614)

Router discovery

The router or switch supports all *RFC 1256, ICMP Router Discovery Messages* as it applies to routers. If this feature is configured, the router or switch sends router advertisements periodically and in response to router solicitations. It does not support the Host Specification section of this RFC.

Benefits

Before an IP host can send an IP packet, it has to know the IP address of a neighbouring router that can forward it to its destination. ICMP Router Discovery messages let routers automatically advertise themselves to hosts. Other methods either require someone to manually keep these addresses up to date, or require DHCP to send the router address, or require the hosts to be able to eavesdrop on whatever routing protocol messages are being used on the LAN.

Router discovery process

The following table summarises what happens when Router Discovery advertisements are enabled for interfaces on the router or switch.

When...	Then...
Router Discovery advertising starts on a router or switch interface because: <ul style="list-style-type: none">- the router or switch starts up, or- advertisements are enabled on the switch or on an interface	the router or switch multicasts a router advertisement and continues to multicast them periodically until router advertising is disabled.
a host starts up	the host may send a router solicitation message.
the router or switch receives a router solicitation	the router or switch multicasts an early router advertisement on the multicast interface on which it received the router solicitation.
a host receives a router advertisement	the host stores the IP address and preference level for the advertisement lifetime.
the lifetime of all existing router advertisements on a host expires	the host sends a router solicitation.

When... (Continued)	Then... (Continued)
a host does not receive a router advertisement after sending a small number of router solicitations	the host waits for the next unsolicited router advertisement
a host needs a default router address	the host uses the IP address of the router or L3 switch with the highest preference level.
Router Discovery advertising is deleted from the physical interface (delete ip advertise command), or the logical interface has advertise set to no (set ip interface command)	the router or switch multicasts a router advertisement with the IP address(es) that stopped advertising, and a lifetime of zero. It continues to periodically multicast router advertisements for other interfaces.
the router or switch receives a router advertisement from another router	the router or switch does nothing but silently discards the message.

Advertisement messages

A *router advertisement* is an ICMP (type 10) message that contains the following:

- in the destination address field of the IP header, the interface's configured advertisement address, either 224.0.0.1 (**all**) or 255.255.255.255 (**limited**).
- in the lifetime field, the interface's configured advertisement lifetime.
- in the Router Address and Preference Level fields, the addresses and preference levels of all the logical interfaces that are set to advertise.

The router or switch does not send router advertisements by default.

Solicitation messages

A *router solicitation* is an ICMP (type 10) message containing:

- source Address: an IP address belonging to the interface from which the message is sent
- destination Address: the configured Solicitation Address, and
- Time-to-Live: 1 if the Destination Address is an IP multicast address; at least 1 otherwise.

Advertisement interval

The router advertisement *interval* is the time between router advertisements. For the first few advertisements sent from an interface (up to 3), the router or switch sends the router advertisements at intervals of at most 16 seconds. After these initial transmissions, it sends router advertisements at random intervals between the minimum and maximum intervals that the user configures, to reduce the probability of synchronization with the advertisements from other routers on the same link. By default the minimum is 450 seconds (7.5 minutes), and the maximum is 600 seconds (10 minutes).

Preference level

The *preference level* is the preference of the advertised address as a default router address relative to other router addresses on the same subnet. By default, all routers and layer 3 switches have the same preference level, zero. While it is entered as a decimal from -2147483648 to 2147483647, it is encoded in router advertisements as a twos-complement hex integer from 0x80000000 to 0x7fffffff. A higher preference level is preferred over a lower value.

Lifetime

The *lifetime* of a router advertisement is how long the information in the advertisement is valid. By default, the lifetime of all advertisements is 1800 seconds (30 minutes).

Configuration procedure

Do the following to configure the router or switch to send router advertisements.

1. Set the physical interface to advertise.

For each physical interface that is to send advertisements, add the interface. In most cases the default advertising parameters work well, but you can change them if required. By default, the router or switch sends advertisements every 7.5 to 10 minutes, with a lifetime of 30 minutes. These settings are likely to work in most situations and not cause extra traffic, even if there are several routers or switches on the LAN. If you change these settings, keep the following proportions:

```
lifetime=3 x maxadvertisementinterval
minadvertisementinterval=0.75 x maxadvertisementinterval
```

To change these settings, use one of the commands:

```
add ip advertise interface=interface [advertisementaddress={all|limited}] [maxadvertisementinterval=4..1800]
[minadvertisementinterval=3..maxadvertisementinterval] [lifetime=maxadvertisementinterval..9000]
set ip advertise interface=interface [advertisementaddress={all|limited}] [maxadvertisementinterval=4..1800]
[minadvertisementinterval=3..maxadvertisementinterval] [lifetime=maxadvertisementinterval..9000]
```

2. Stop advertising on other logical interfaces.

By default, logical interfaces are set to advertise if their physical interface is set to advertise. If the physical interface has more than one logical interface (IP multihoming), and you only want some of them to advertise, set the other logical interfaces not to advertise with one of the commands:

```
add ip interface=interface ipaddress={ipadd|dhcp} advertise=no [other-ip-parameters]  
set ip interface=interface advertise=no [other-ip-parameters]
```

3. Set preference levels.

By default, every logical interface has the same preference for becoming a default router (mid range, 0). To give a logical interface a higher preference, increase **preferencelevel**. To give it a lower preference, decrease this value. If it should never be used as a default router, set it to **notdefault**.

```
add ip interface=interface ipaddress={ipadd|dhcp} preferencelevel={-2147483648..2147483647|notdefault} [other-ip-parameters]  
set ip interface=interface  
[preferencelevel={-2147483648..2147483647|notdefault}] [other-ip-parameters]
```

4. Enable advertising.

To enable router advertisements on all configured advertising interfaces, use the command:

```
enable ip advertise
```

5. Check advertise settings.

To check the router advertisement settings, use the command:

```
show ip advertise
```

STP and MSTP debugging enhancements (CR00016978)

Debugging command and output enhancements

STP and MSTP debugging have been enhanced in the following ways:

- A new STP and MSTP debugging option turns on real-time switch port state debugging. This option displays a message every time STP/MSTP asks for the state of a port to be changed. To enable the new debugging, use one of the commands:

```
enable stp[={stp-name|ALL}] debug=swi
```

```
enable mstp debug=swi
```

The output takes the form “<timestamp> <port> <new state>”. For example, the output “13:37:47/6.4/Discarding” shows that port 6.4 moved in to the discarding state at 13:37:47.

- New switch debugging options report the same output as the new STP/MSTP debug option, but displays the output when the STP/MSTP state changes within the switching module, instead of within the STP/MSTP module. Therefore, the STP/MSTP debugging shows the change that STP/MSTP asked for and the switch debugging shows the change that switching made. These two changes should be compatible. To enable the new switch debugging, use the command:

```
enable switch debug={stp|mstp}
```

- A new **tonly** parameter limits message debugging so that an incoming or outgoing message is only displayed if it is a topology change message (the TC-flag is set within the message). This is useful when debugging IGMP topology change notification. To turn this feature on and off, use one of the commands:

```
enable stp[={stp-name|ALL}] debug=msg tonly={on|off|yes|no}
```

```
enable mstp debug=msg tonly={on|off|yes|no}
```

The default is **off**.

- All STP and MSTP debugging output is now time-stamped.

New *show* commands

The following new commands display the current port states (in hardware) of all ports that are taking part in STP or MSTP:

```
show switch stp
show switch mstp
```

The following example shows the output of the **show switch stp** command.

```
Switch STP Port State Information at 12:09:52:
ST   Port      State
--   ----      -
0    2          Fo
0    3          Fo
0    5          Bl
0    6          Li
```

The following example shows the output of the **show switch mstp** command.

```
Switch MSTP Port State Information
Switch STP Port State Information at 04:50:37:
ST   Port      State
--   ----      -
1    33         Fo
1    48         Fo
2    33         Fo
2    48         Fo
3    33         Fo
3    48         Fo
```


The following table lists the fields in this output.

Parameter	Meaning
ST	The ID number of the Spanning Tree that the port belongs to.
Port	The switch port whose state is displayed.
State	The STP state of the port.
Bl	Blocking: forwarding disabled, learning disabled, BPDUs received
Li	Listening: forwarding disabled, learning disabled, BPDUs received (only on AT-9800 series switches)
Le	Learning: forwarding disabled, learning enabled, BPDUs received
Fo	Forwarding: forwarding enabled, learning enabled, BPDUs received
Di	Disabled: forwarding disabled, learning disabled, BPDUs discarded

Acting on traffic destined for a particular DHCP client (CR00017018)

This enhancement enables you to act on traffic that is received on an uplink port and is destined for a particular DHCP client. It expands the classifier functionality so that the switch can use DHCP snooping records to determine which traffic is destined for each client. Once the classifier has identified the traffic, you can apply a QoS policy or hardware filters to it.

The enhancement applies to AT-8948, x900-48, and AT-9900 series switches.

For example, you can use the new functionality to track how much traffic each user receives via an uplink port. This enables you to track traffic usage at the uplink port, even if destination IP addresses are dynamically assigned by DHCP and traffic for multiple users is in the same VLAN.

To configure such tracking:

6. Configure DHCP snooping.

7. Create the required classifiers.

For each DHCP client, create a classifier using the following new options:

```
create classifier=id ipaddress=dhcpsnooping snooport=port-number snoopvlan=vlan-id
```

The **dhcpsnooping** option for the **ipaddress** parameter causes the switch to dynamically create appropriate classifiers when DHCP snooping deems that an appropriate DHCP lease event has occurred.

The **snooport** parameter specifies the switch port that traffic egresses for the target DHCP client.

The **snoopvlan** parameter specifies the VLAN for traffic to that client.

8. Put the classifiers into a QoS heirarchy.

9. Apply the QoS policy to the uplink port.

10. Use the traffic class counters to see how much traffic is destined for each client.

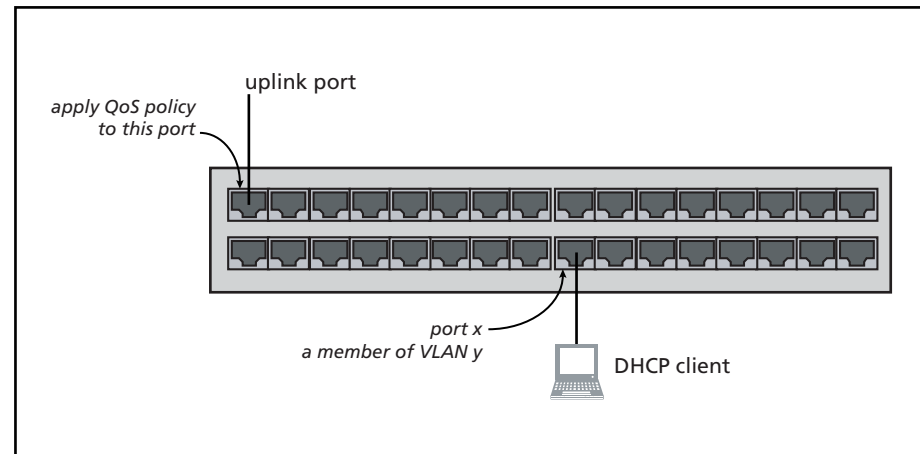
The new options have also been added to the **set classifier** command and output of the **show classifier** command.

Example

For example, consider the following figure. In this example, the QoS policy on the uplink port includes the following classifier:

```
create classifier=1 ip=dhcp Snooping snoopport=x snoopvlan=y
```

When the client receives a DHCP lease, all traffic that comes in through the uplink port and is destined for the client will match classifier 1.

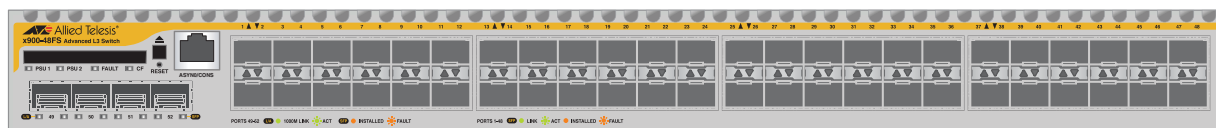


Support for the new x900-48FS switch (CR00016662)

The x900-48FS is a new model in the x900 Series of layer 3 gigabit and fast Ethernet switches. Its key features are:

- Multi-layer Fast Ethernet switch
- 48-port 100BASE-X SFP sockets, 100 Mbps, full or half duplex
- 4-port 1000BASE-X SFP uplink sockets, 1000 Mbps, full duplex
- Support for hot-swappable SFP modules
- Hot-swappable, load sharing PSUs
- 1U height, rack-mountable
- Non-blocking Layer 2 and Layer 3 IP switching
- IPv6-ready hardware for accelerated unicast and multicast routing
- 4096 Layer 2 multicast entries
- 1024 Layer 3 IPv4 multicast entries
- 4096 logical IPv6 interfaces
- 32MBytes of fixed flash
- 256MBytes of Synchronous DRAM, expandable to 512MBytes with DIMM
- CompactFlash slot for hot-swappable expansion of flash memory up to 128MBytes

x900-48FS front panel



For more information about the x900 Series and expansion options, see the Hardware Reference. The Hardware Reference is available from www.alliedtelesis.co.nz/documentation/manuals.html.

IGMP snooping fast leave in multiple host mode (CR00017482)

The IGMP snooping fast leave option has been enhanced, to make it available when multiple clients are attached to a single port on the snooping switch. Fast leave now has two modes available:

- **multiple host mode**—the new feature. In multiple host mode, the snooper tracks which clients are joined to a given IP multicast group on a given port. As soon as the last client leaves a group on a port, the snooper shuts off the multicast to that port.
- **single host mode**—the existing functionality. In single host mode, as soon as the snooper receives a leave message for a group on a port, it shuts off the multicast. This mode assumes that there are no other clients on the port that are still interested in receiving the multicast, so is suitable only when clients are directly attached to the snooper.

To specify the new multiple mode, use the command:

```
set igmpsnooping vlan={vlan-name|1..4094|all} fastleave=multiple
```

To specify single mode, use either of the commands:

```
set igmpsnooping vlan={vlan-name|1..4094|all} fastleave=single
```

```
set igmpsnooping vlan={vlan-name|1..4094|all} fastleave=on
```

The command **show igmpsnooping vlan** has also been enhanced. The new command syntax is:

```
show igmpsnooping vlan={vlan-name|1..4094|all} [group={multicast-ip-address|allgroups}] [detail]
```

The **group** parameter lets you display information for only one group or for only the All Groups port (the **allgroups** option).

The **detail** parameter displays more detailed information, including expiry times for each port, and in the case of multiple host fast leave mode, the list of hosts on a port. The following example shows this.

```
IGMP Snooping
-----
Status ..... Enabled
Disabled All-groups ports ..... None

Vlan Name (vlan id) ..... default (1)
Fast Leave ..... Multiple Host Topology
Query Solicitation ..... Off
Static Router Ports ..... None
Group List ..... 2 groups

  Group 224.0.1.22                                Timeout in 256 secs
    Port 24                                       Timeout in 257 secs
      Hosts: 1
        00-00-cd-27-be-f5 (172.20.176.200)      Timeout in 257 secs

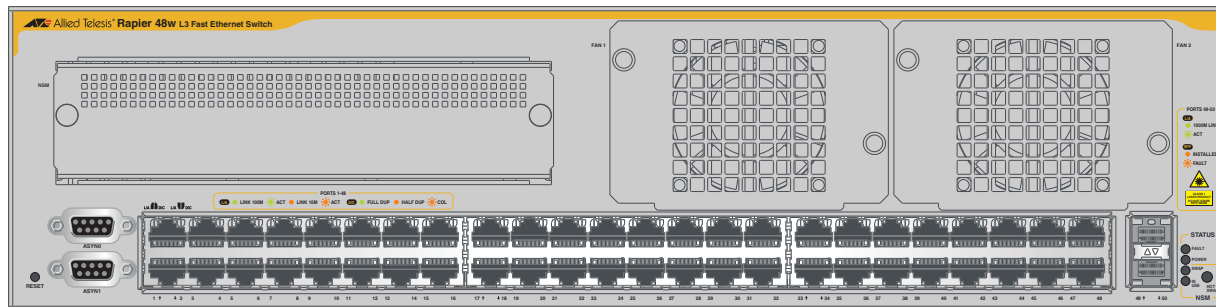
  Group 239.255.255.250                          Timeout in 258 secs
    Port 24                                       Timeout in 259 secs
      Hosts: 1
        00-00-cd-27-be-f5 (172.20.176.200)      Timeout in 259 secs
```

Support for the new Rapier 48w switch

The Rapier 48w is a new model in the Rapier Series of layer 3 gigabit and fast Ethernet switches. Its key features are:

- 48-port 10BASE-T/100BASE-TX (RJ-45 connectors)
- Two 1000BASE SFP ports
- Two asynchronous serial console ports with DB9 connectors
- One Network Service Module bay, with support for various WAN interface cards
- Auto-negotiating Layer 3 Managed Switch
- Enhanced switching core
- Replaceable air filters and fan-only modules (FOMs) for NEBS applications

Rapier 48w front panel



Rapier 48w rear panel



For more information about the Rapier Series and expansion options, see the Hardware Reference. The Hardware Reference is available from www.alliedtelesis.co.nz/documentation/manuals.html.

Backing up the configuration with SNMP (CR00016221)

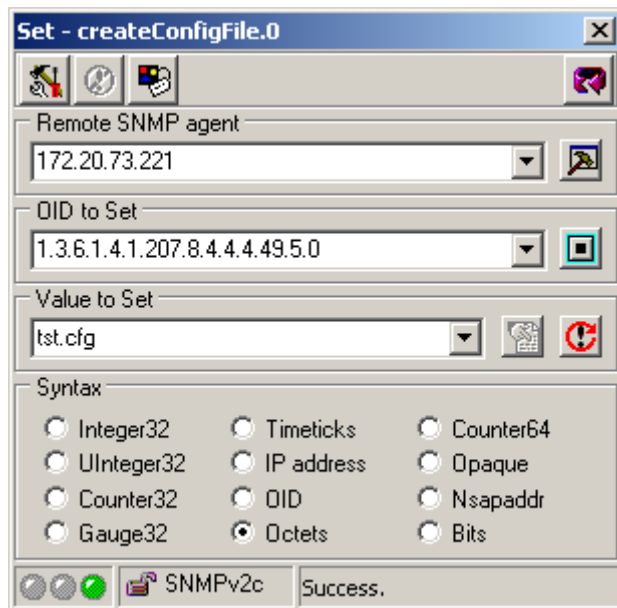
With this enhancement, you can use SNMP to:

- set parameters for uploading files from the router or switch, and
- upload files to a TFTP server

SNMP already lets you save the current configuration to a file on the router or switch. You can use this with the new options to back up the configuration to a TFTP server. To do this, perform the following steps.

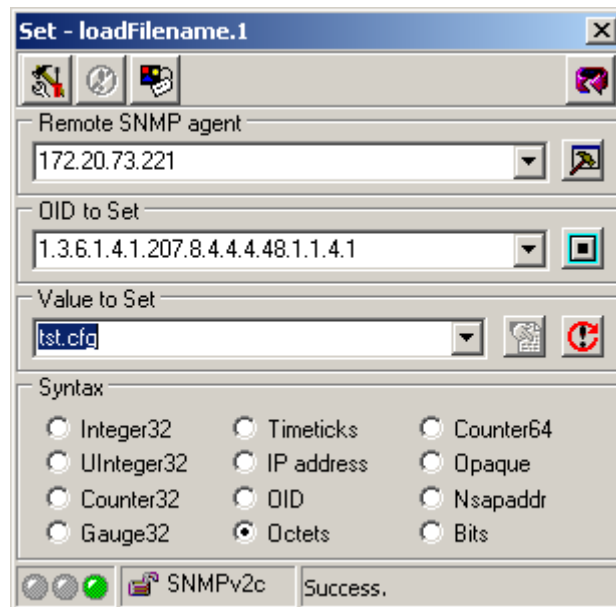
1. Save the configuration

To save the current configuration, use SNMP SET createConfigFile. The following screenshot shows this for a file called tst.cfg.



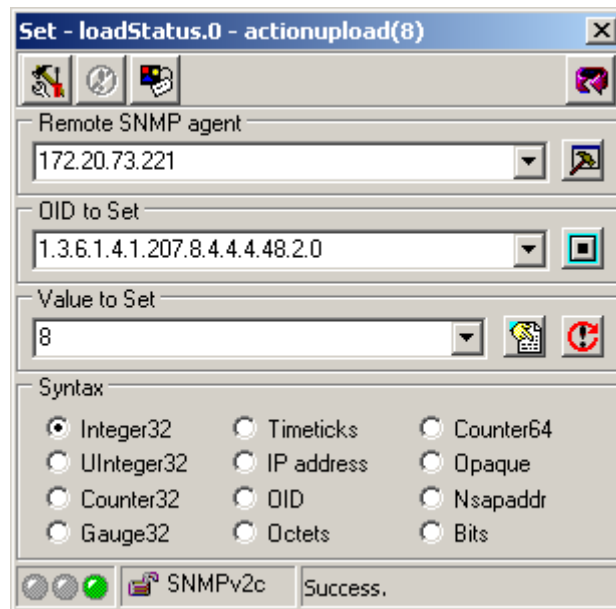
2. Set the load parameters

To specify the server IP address, use SNMP SET loadServer. To set the filename, use SNMP SET loadFilename. The following screenshot shows setting the filename to tst.cfg.



3. Upload the file

To upload the file, use SNMP SET loadStatus and set it to a value of 8. The following screenshot shows this.



SNMP ASN.01 BER Padding (CR00016523)

This enhancement enables you to specify whether SNMP adds 0x00 padding when the most significant 9 bits of an object's value are all 1, or whether the encoding follows the ASN.01 BER rule, which cuts off the most significant byte of 0xff. This setting has an impact on all integer type MIB objects, including 32 bit and 64 bit counter objects.

To add the padding, use the command:

```
set snmp asnberpadding={on|yes|true}
```

To use the ASN.01 BER rule, which is the default, use the command:

```
set snmp asnberpadding={off|no|false}
```

The following table lists examples.

Bits	Value (decimal)	Value (hex)	asnberpadding setting	Encoding
counter32	4289592837	0xFFADFE05	on	41 05 00 ff ad fe 05
			off	41 03 ad fe 05
counter64	18410715280977201498	0xFF800000ff80895A	on	46 09 00 ff 80 00 00 ff 80 89 5a
			off	46 07 80 00 00 ff 80 89 5a

To see whether or not padding is added, use the command:

```
show snmp
```

and check the new “ASN.01 BER Padding” field.